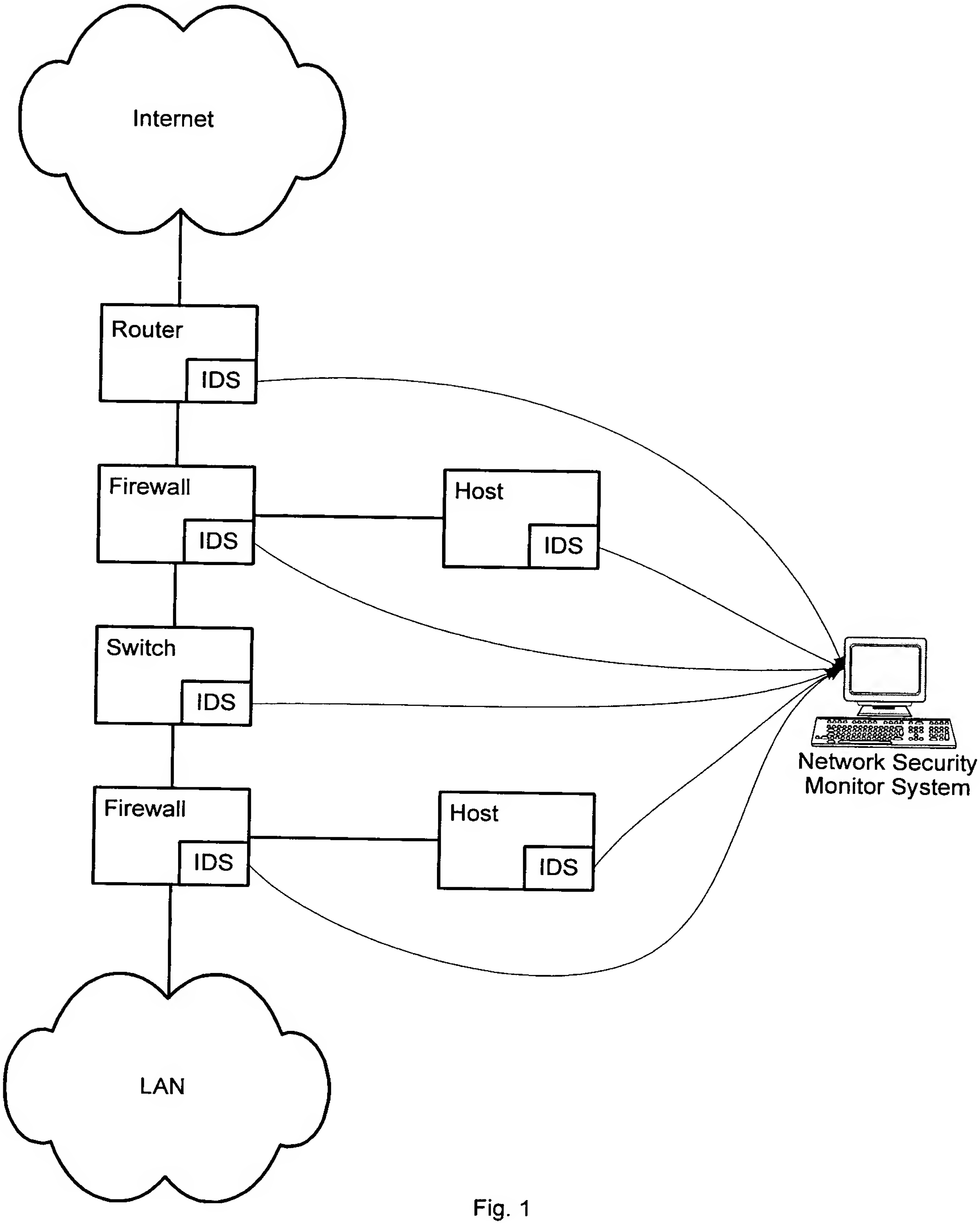

Internet
Router
IDS
Firewall
IDS
Host
IDS
Switch
IDS
Firewall
IDS
Host
IDS
Network Security Monitor System
LAN

Fig. 1

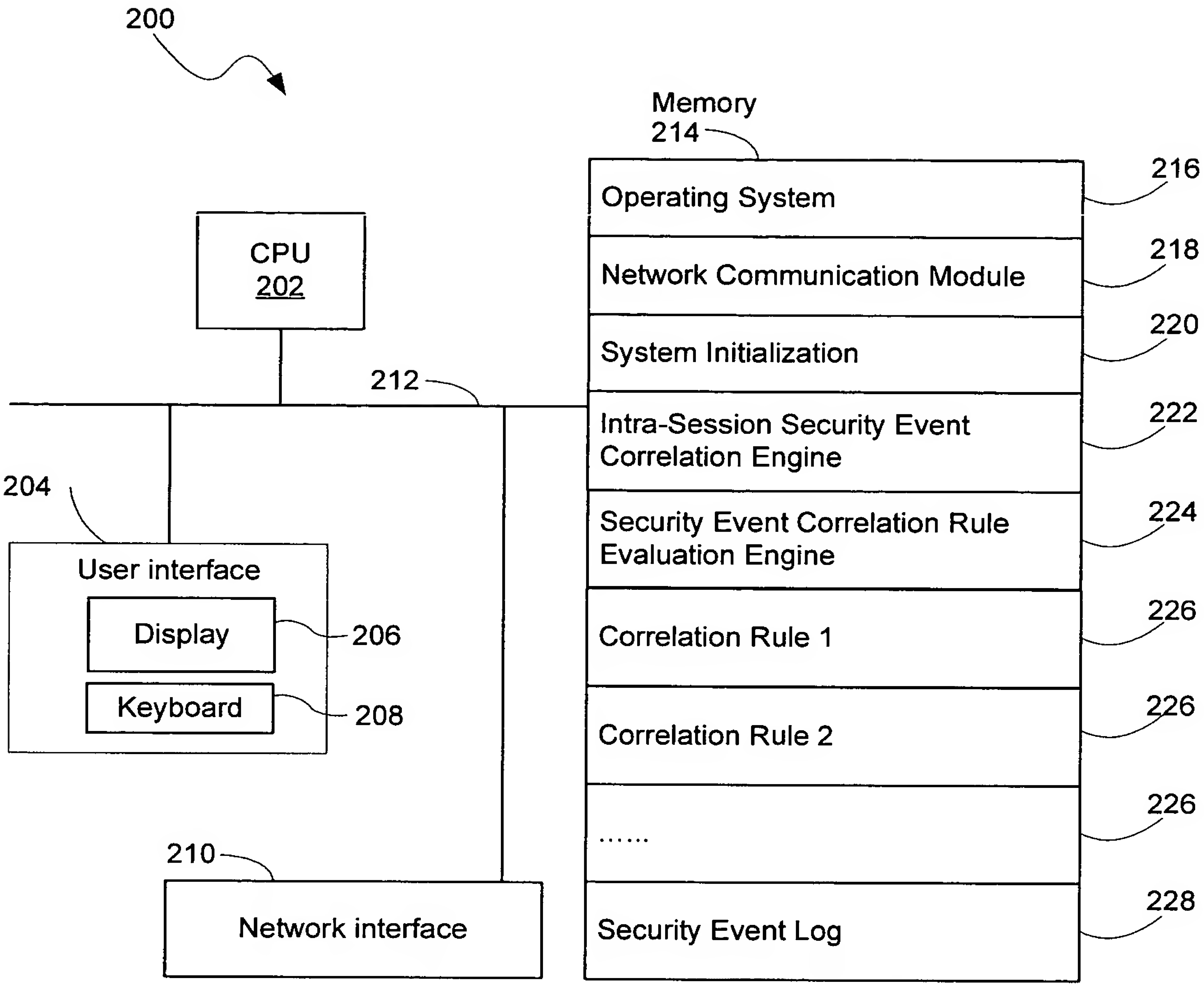

200
Memory
214
CPU
202
212
216
Operating System
218
Network Communication Module
220
System Initialization
222
Intra-Session Security Event Correlation Engine
224
Security Event Correlation Rule Evaluation Engine
226
Correlation Rule 1
226
Correlation Rule 2
226
……
228
Security Event Log
204
User interface
Display
206
Keyboard
208
210
Network interface

Fig. 2

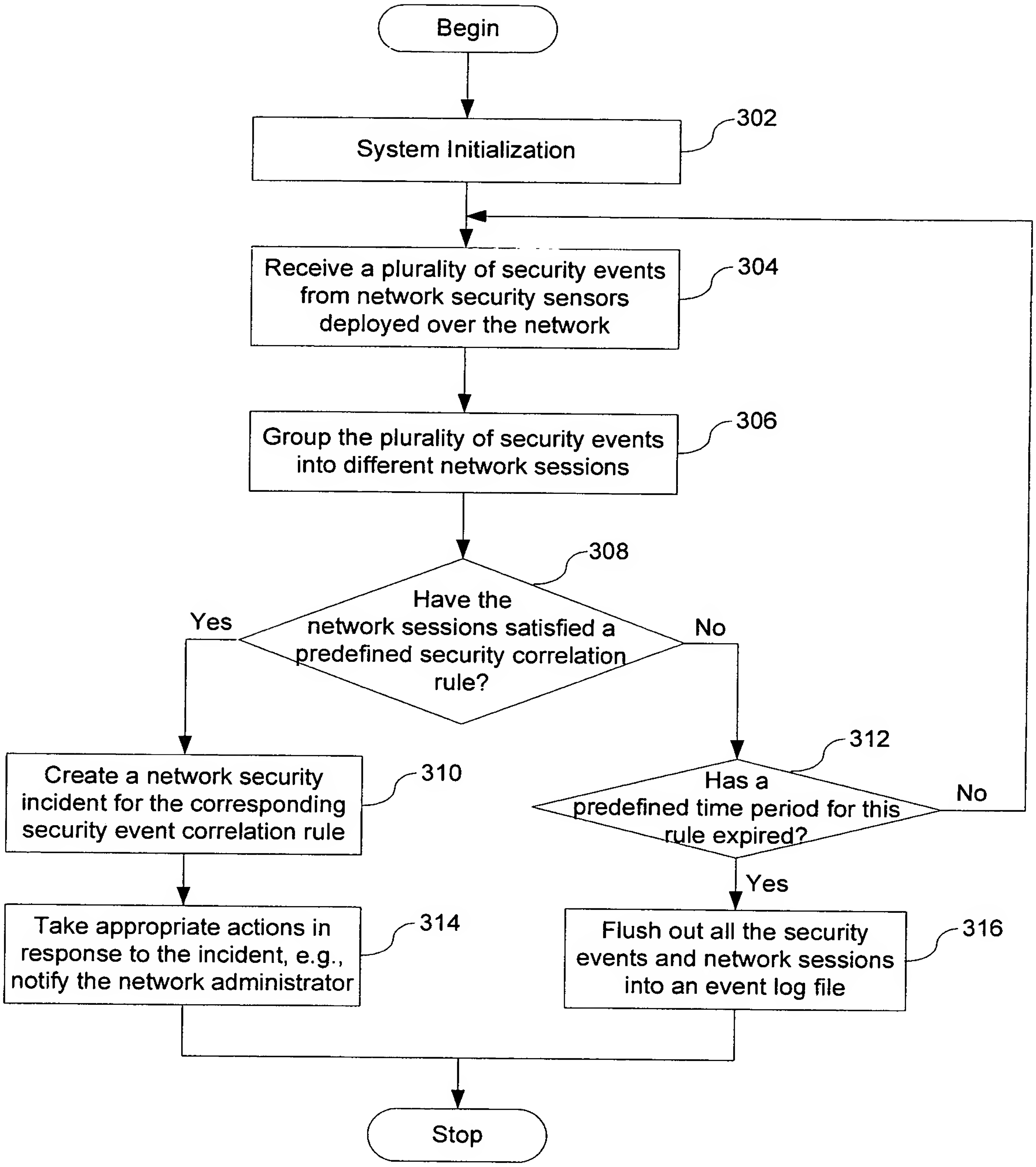

Begin
System Initialization
302
Receive a plurality of security events from network security sensors deployed over the network
304
Group the plurality of security events into different network sessions
306
308
Have the network sessions satisfied a predefined security correlation rule?
Yes
No
Create a network security incident for the corresponding security event correlation rule
310
312
Has a predefined time period for this rule expired?
No
Yes
Take appropriate actions in response to the incident, e.g., notify the network administrator
314
Flush out all the security events and network sessions into an event log file
316
Stop

Fig. 3

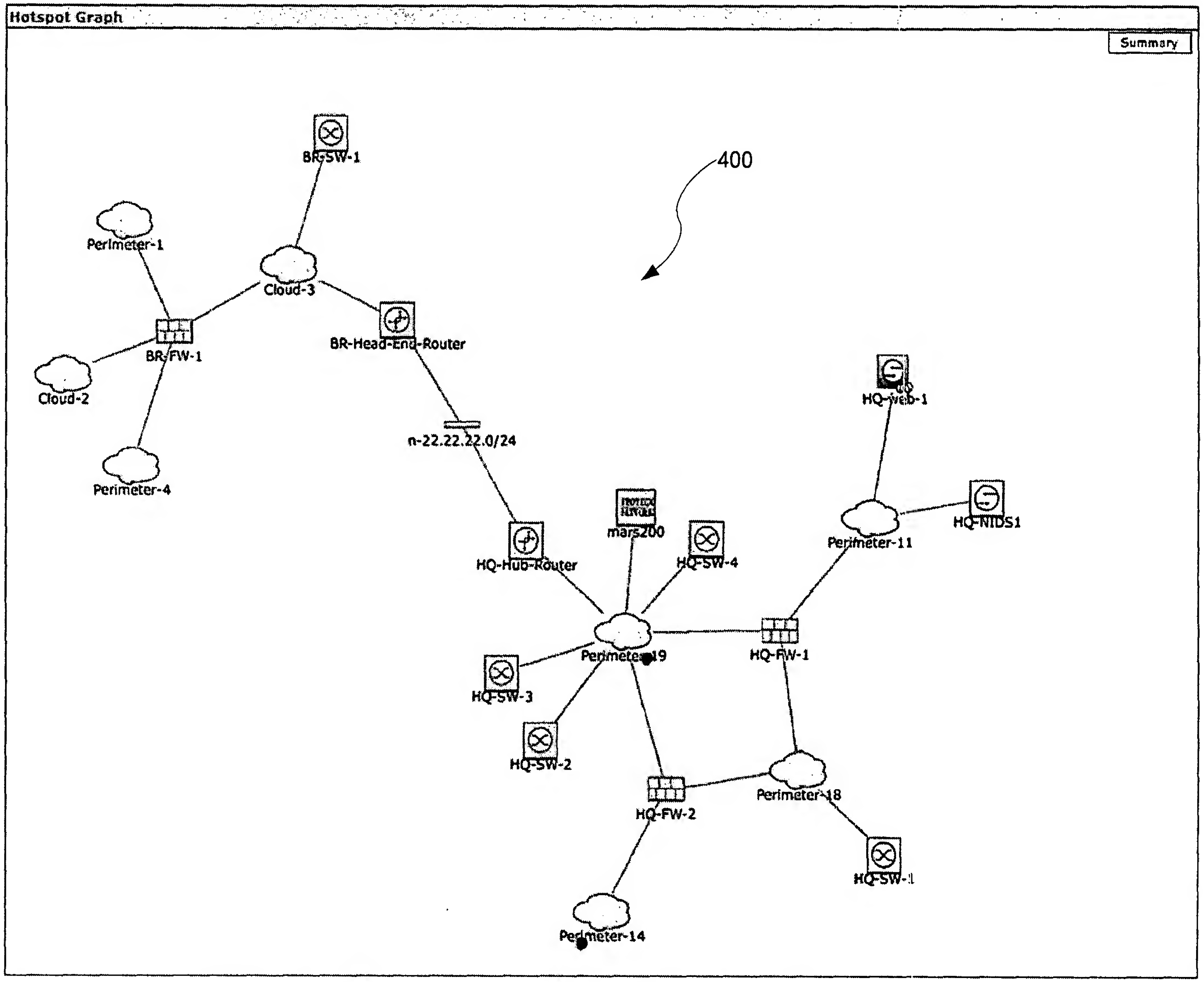

Hotspot Graph
Summary
400
BR-SW-1
Perimeter-1
Cloud-3
BR-FW-1
Cloud-2
Perimeter-4
BR-Head-End-Router
n-22.22.22.0/24
HQ-Hub-Router
mars200
HQ-SW-4
HQ-Web-1
HQ-NIDS1
Perimeter-11
Perimeter-19
HQ-FW-1
HQ-SW-3
HQ-SW-2
HQ-FW-2
Perimeter-18
HQ-SW-1
Perimeter-14

Fig. 4(A)

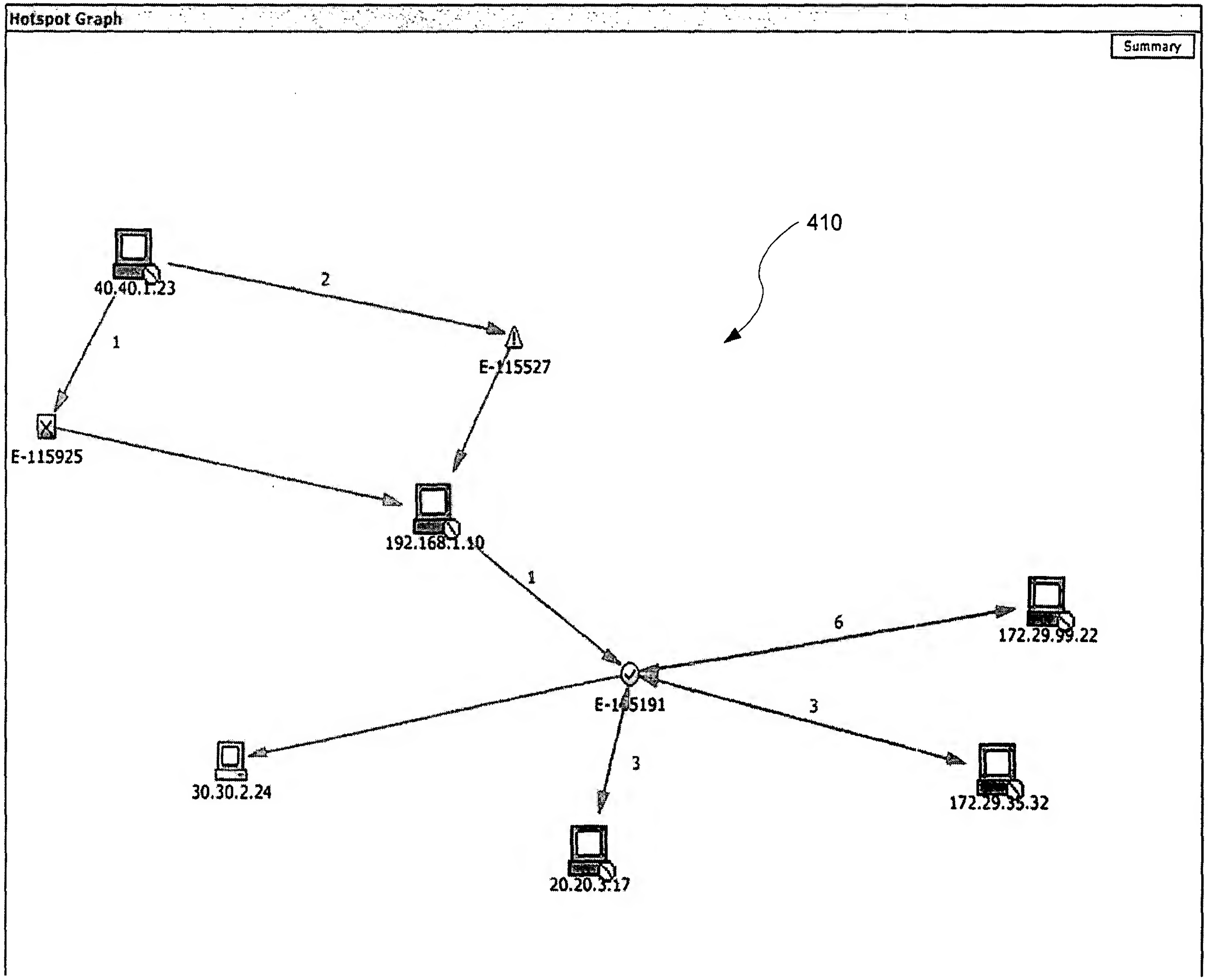

Hotspot Graph
Summary
410
40.40.1.23
2
1
E-115527
E-115925
192.168.1.10
1
6
172.29.99.22
E-115191
3
3
30.30.2.24
20.20.3.17
172.29.35.32

Fig. 4(B)

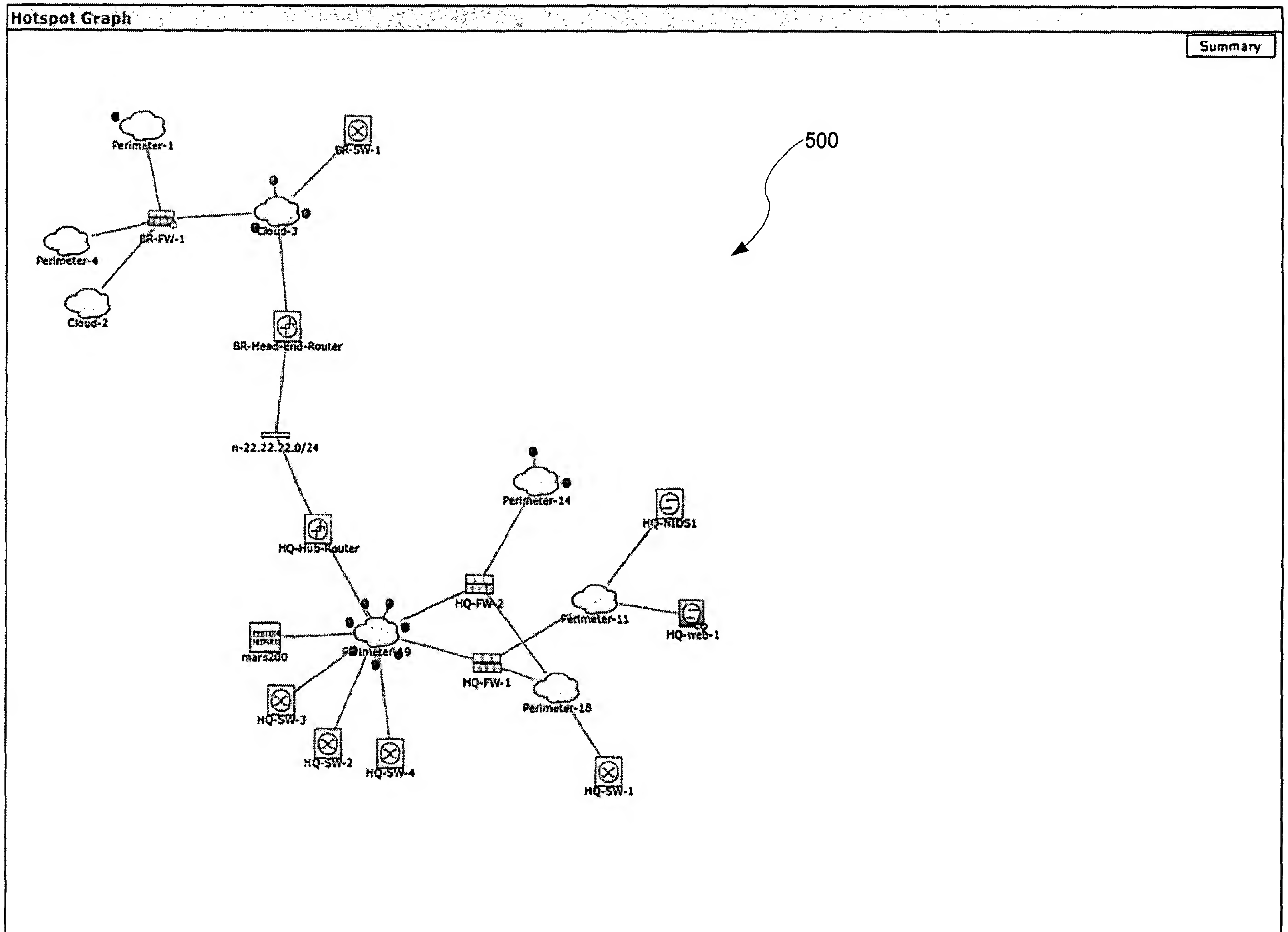

Hotspot Graph
Summary
500
Perimeter-1
BR-SW-1
BR-FW-1
Cloud-3
Perimeter-4
Cloud-2
BR-Head-End-Router
n-22.22.22.0/24
Perimeter-14
HQ-NIDS1
HQ-Hub-Router
HQ-FW-2
Perimeter-11
HQ-web-1
mars200
Perimeter-19
HQ-FW-1
Perimeter-18
HQ-SW-3
HQ-SW-2
HQ-SW-4
HQ-SW-1

Fig. 5(A)

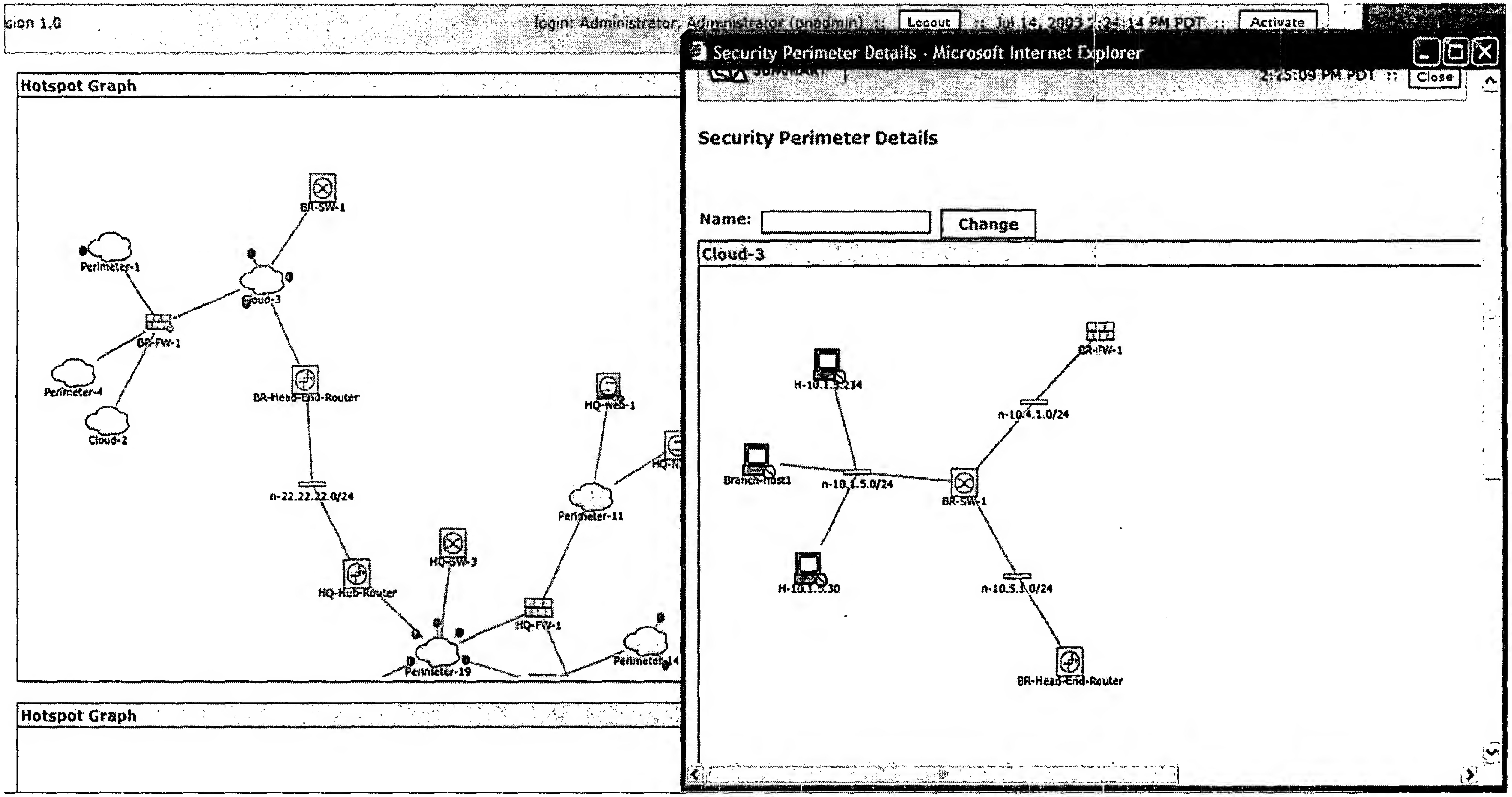
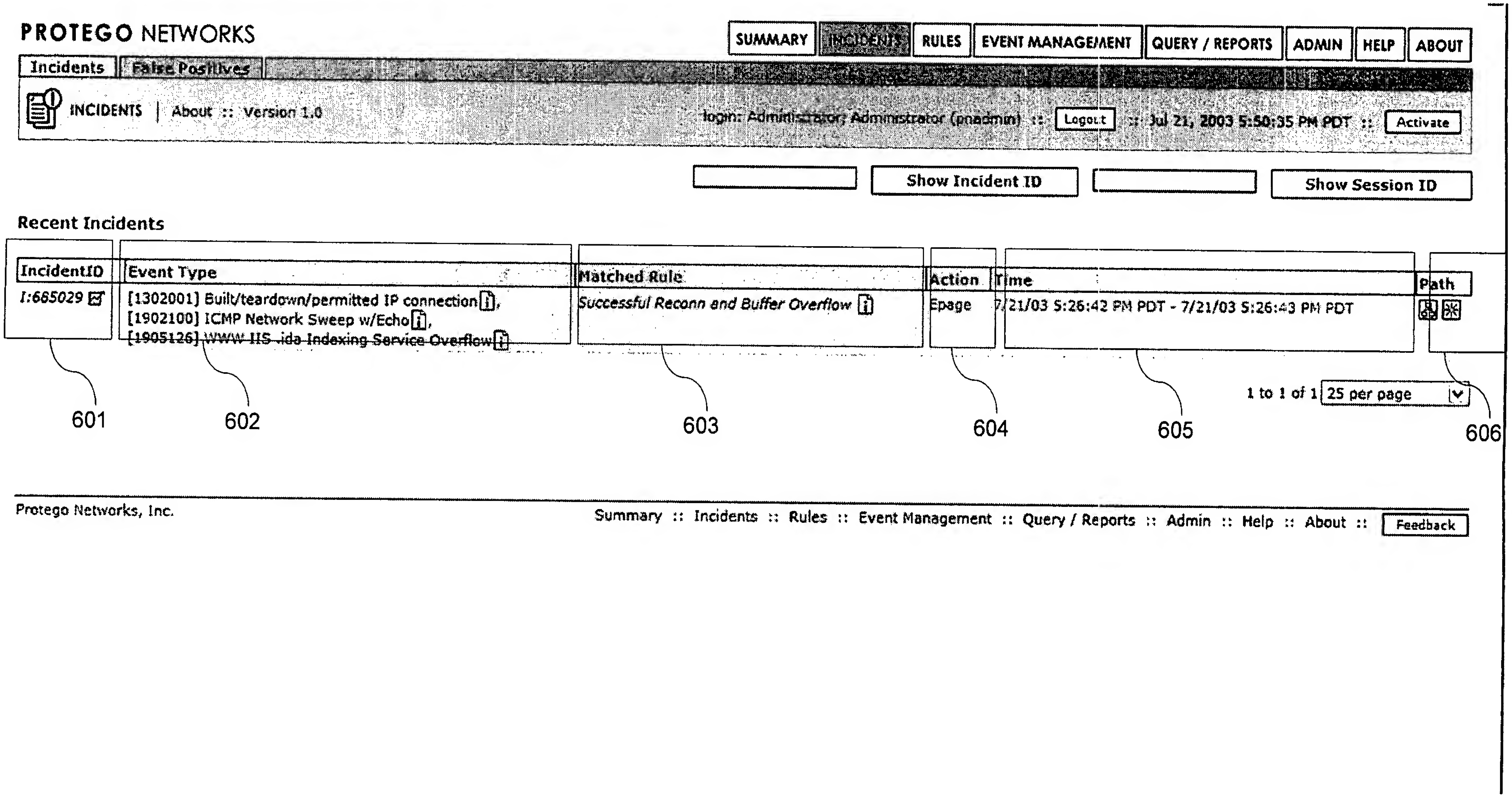
sion 1.0
login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14, 2003 2:24:14 PM PDT :: Activate
Hotspot Graph
BR-SW-1
Perimeter-1
Cloud-3
BR-FW-1
Perimeter-4
Cloud-2
BR-Head-End-Router
n-22.22.22.0/24
HQ-Hub-Router
HQ-SW-3
Perimeter-19
HQ-FW-1
Perimeter-11
HQ-Web-1
HQ-N
Perimeter-14
Hotspot Graph
Security Perimeter Details - Microsoft Internet Explorer
2:25:09 PM PDT :: Close
Security Perimeter Details
Name:
Change
Cloud-3
H-10.1.5.234
Branch-host1
n-10.1.5.0/24
H-10.1.5.30
BR-SW-1
n-10.4.1.0/24
BR-FW-1
n-10.5.1.0/24
BR-Head-End-Router

Fig. 5(B)

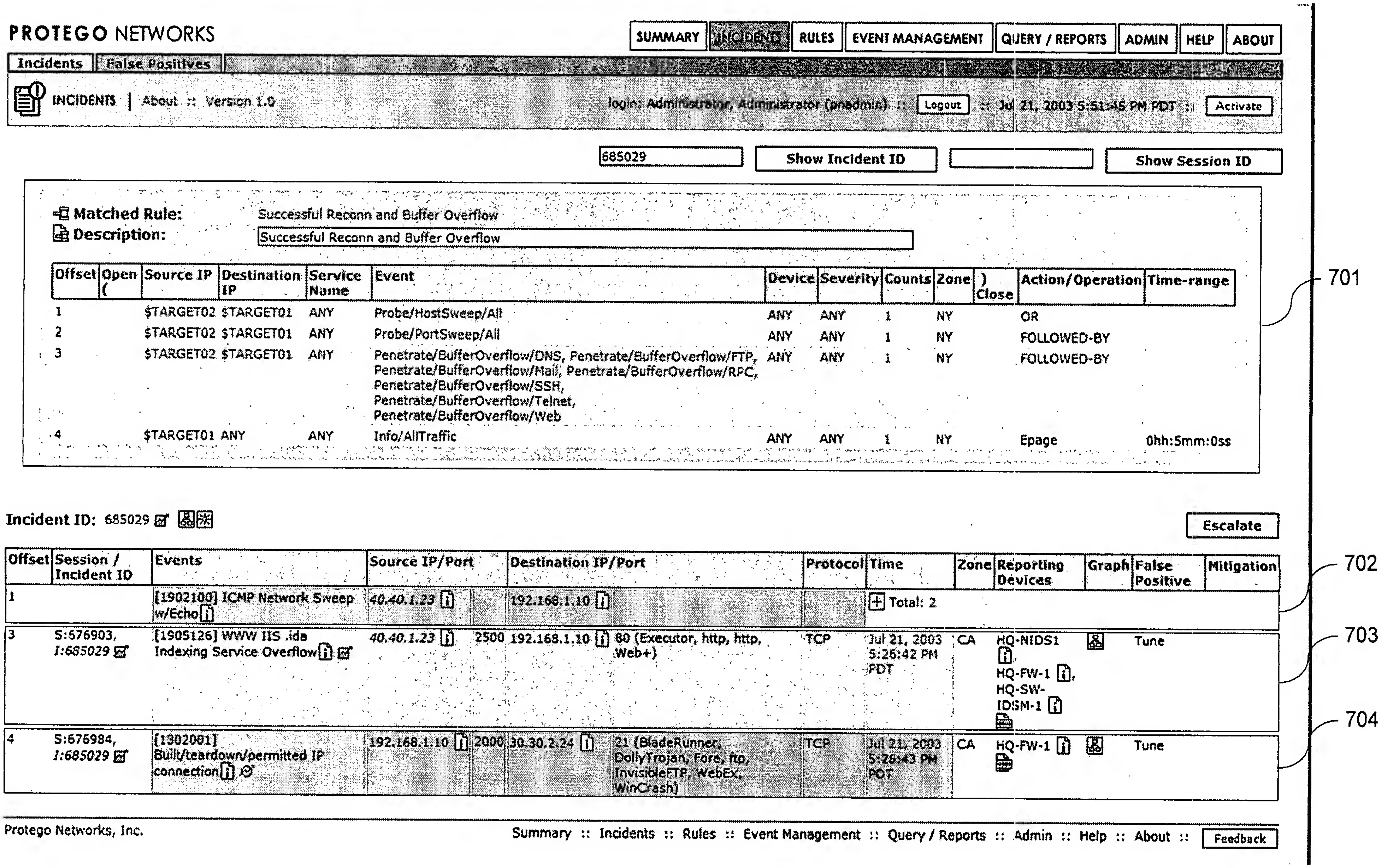


Recent Incidents

IncidentID	Event Type	Matched Rule	Action	Time	Path
I:685029	[1302001] Built/teardown/permitted IP connection, [1902100] ICMP Network Sweep w/Echo, [1905126] WWW IIS .ida Indexing Service Overflow	*Successful Reconn and Buffer Overflow*	Epage	7/21/03 5:26:42 PM PDT - 7/21/03 5:26:43 PM PDT	

1 to 1 of 1
25 per page
601
602
603
604
605
606
Protego Networks, Inc.
Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::
Feedback

Fig. 6


PROTEGO NETWORKS
SUMMARY
INCIDENTS
RULES
EVENT MANAGEMENT
QUERY / REPORTS
ADMIN
HELP
ABOUT
Incidents
False Positives
INCIDENTS | About :: Version 1.0
login: Administrator, Administrator (pnadmin) :: Logout :: Jul 21, 2003 5:51:45 PM PDT :: Activate
Show Incident ID
Show Session ID
Escalate
Protego Networks, Inc.
Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback
701
702
703
704

685029

Matched Rule: Successful Reconn and Buffer Overflow

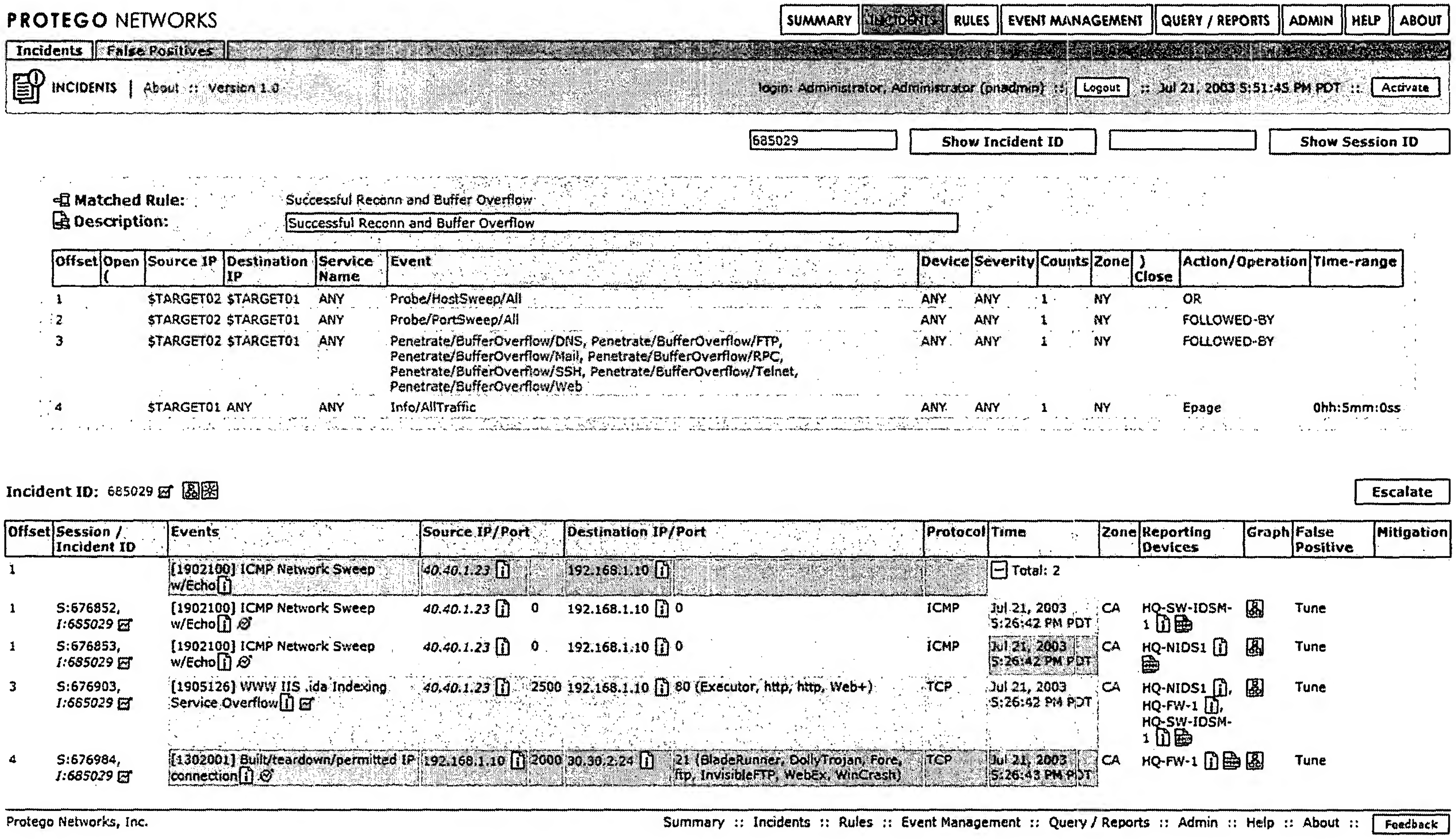
Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All	ANY	ANY	1	NY		OR	
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All	ANY	ANY	1	NY		FOLLOWED-BY	
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web	ANY	ANY	1	NY		FOLLOWED-BY	
4		$TARGET01	ANY	ANY	Info/AllTraffic	ANY	ANY	1	NY		Epage	0hh:5mm:0ss

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10		⊞ Total: 2					
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23 2500	192.168.1.10 80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10 2000	30.30.2.24 21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Fig. 7



Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All	ANY	ANY	1	NY		OR	
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All	ANY	ANY	1	NY		FOLLOWED-BY	
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web	ANY	ANY	1	NY		FOLLOWED-BY	
4		$TARGET01	ANY	ANY	Info/AllTraffic	ANY	ANY	1	NY		Epage	0hh:5mm:0ss

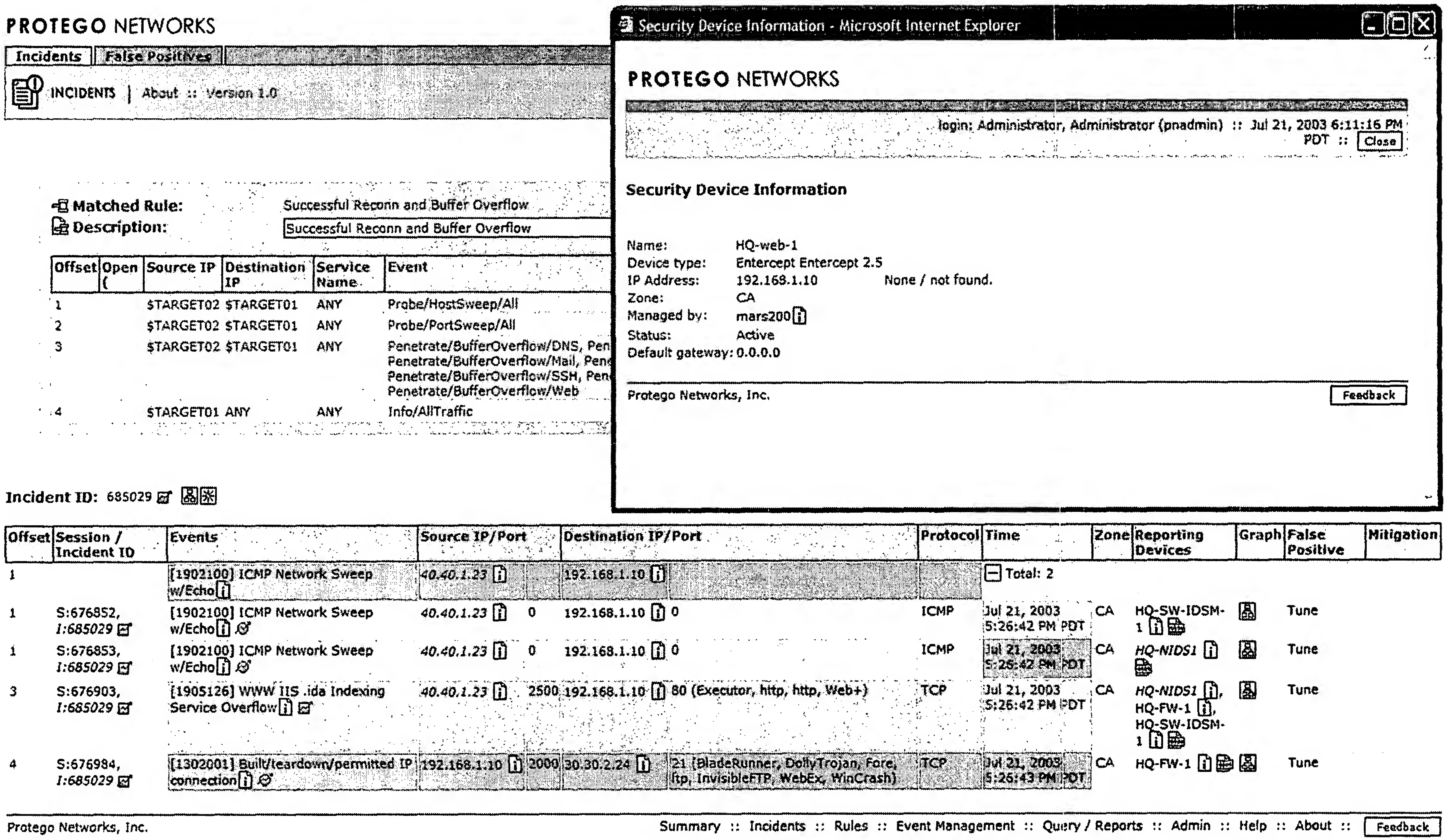
Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			Total: 2					
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::
Feedback

Fig. 8



Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Pen Penetrate/BufferOverflow/Mail, Pen Penetrate/BufferOverflow/SSH, Pen Penetrate/BufferOverflow/Web
4		$TARGET01	ANY	ANY	Info/AllTraffic

login: Administrator, Administrator (pnadmin) :: Jul 21, 2003 6:11:16 PM PDT :: Close

Security Device Information

Name: HQ-web-1
Device type: Entercept Entercept 2.5
IP Address: 192.168.1.10 None / not found.
Zone: CA
Managed by: mars200
Status: Active
Default gateway: 0.0.0.0

Protego Networks, Inc.

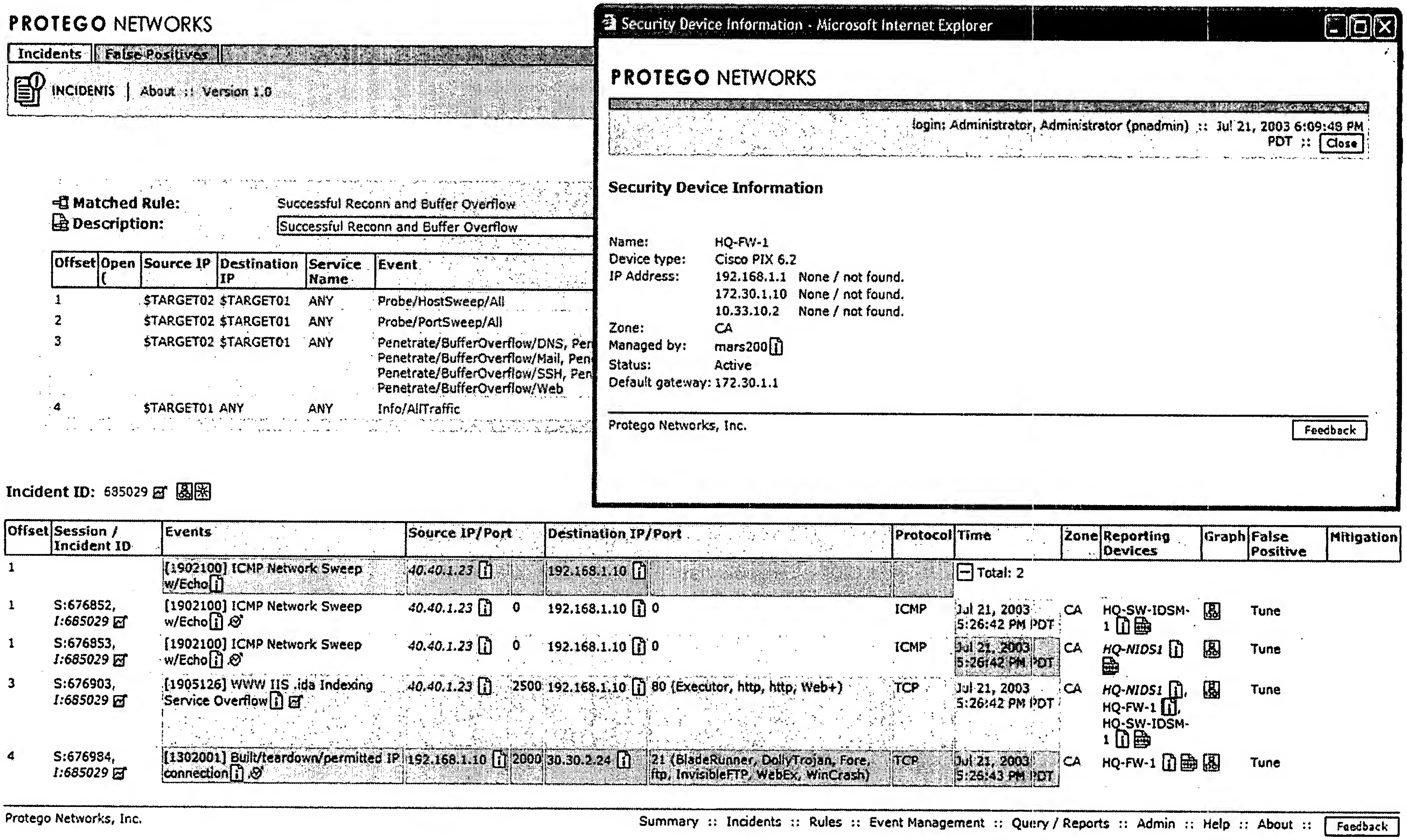
Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			⊟ Total: 2					
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 9



PROTEGO NETWORKS

Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Per Penetrate/BufferOverflow/Mail, Pen Penetrate/BufferOverflow/SSH, Pen Penetrate/BufferOverflow/Web
4		$TARGET01	ANY	ANY	Info/AllTraffic

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 21, 2003 6:09:48 PM PDT :: Close

Security Device Information

Name:	HQ-FW-1
Device type:	Cisco PIX 6.2
IP Address:	192.168.1.1 None / not found. 172.30.1.10 None / not found. 10.33.10.2 None / not found.
Zone:	CA
Managed by:	mars200
Status:	Active
Default gateway:	172.30.1.1

Protego Networks, Inc.

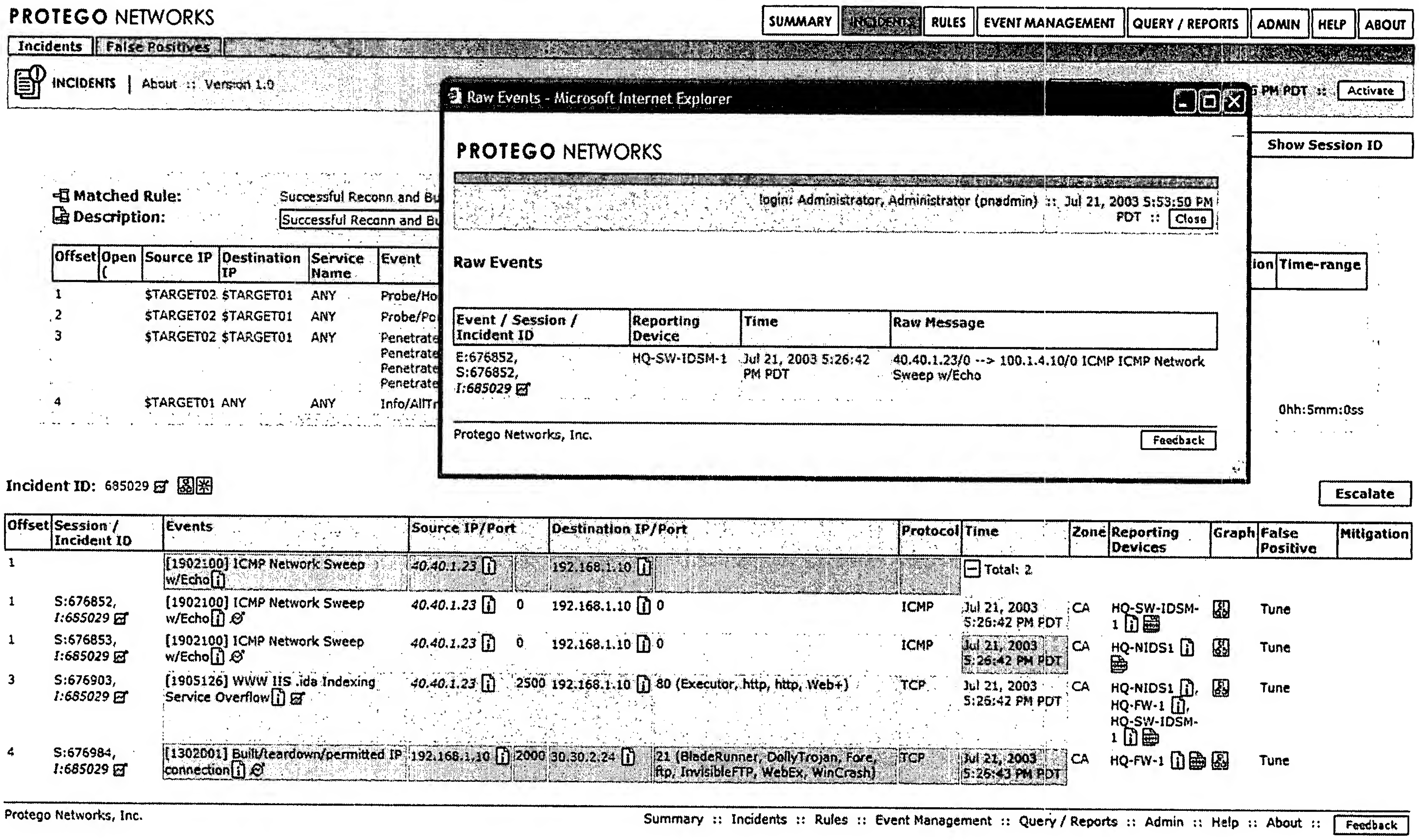
Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			Total: 2					
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 10



PROTEGO NETWORKS

Matched Rule: Successful Reconn and Bu

Description: Successful Reconn and Bu

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/Ho
2		$TARGET02	$TARGET01	ANY	Probe/Po
3		$TARGET02	$TARGET01	ANY	Penetrate Penetrate Penetrate Penetrate
4		$TARGET01	ANY	ANY	Info/AllTr

ion	Time-range
	0hh:5mm:0ss

Raw Events - Microsoft Internet Explorer

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 21, 2003 5:53:50 PM PDT :: Close

Raw Events

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:676852, S:676852, I:685029	HQ-SW-IDSM-1	Jul 21, 2003 5:26:42 PM PDT	40.40.1.23/0 --> 100.1.4.10/0 ICMP ICMP Network Sweep w/Echo

Protego Networks, Inc.

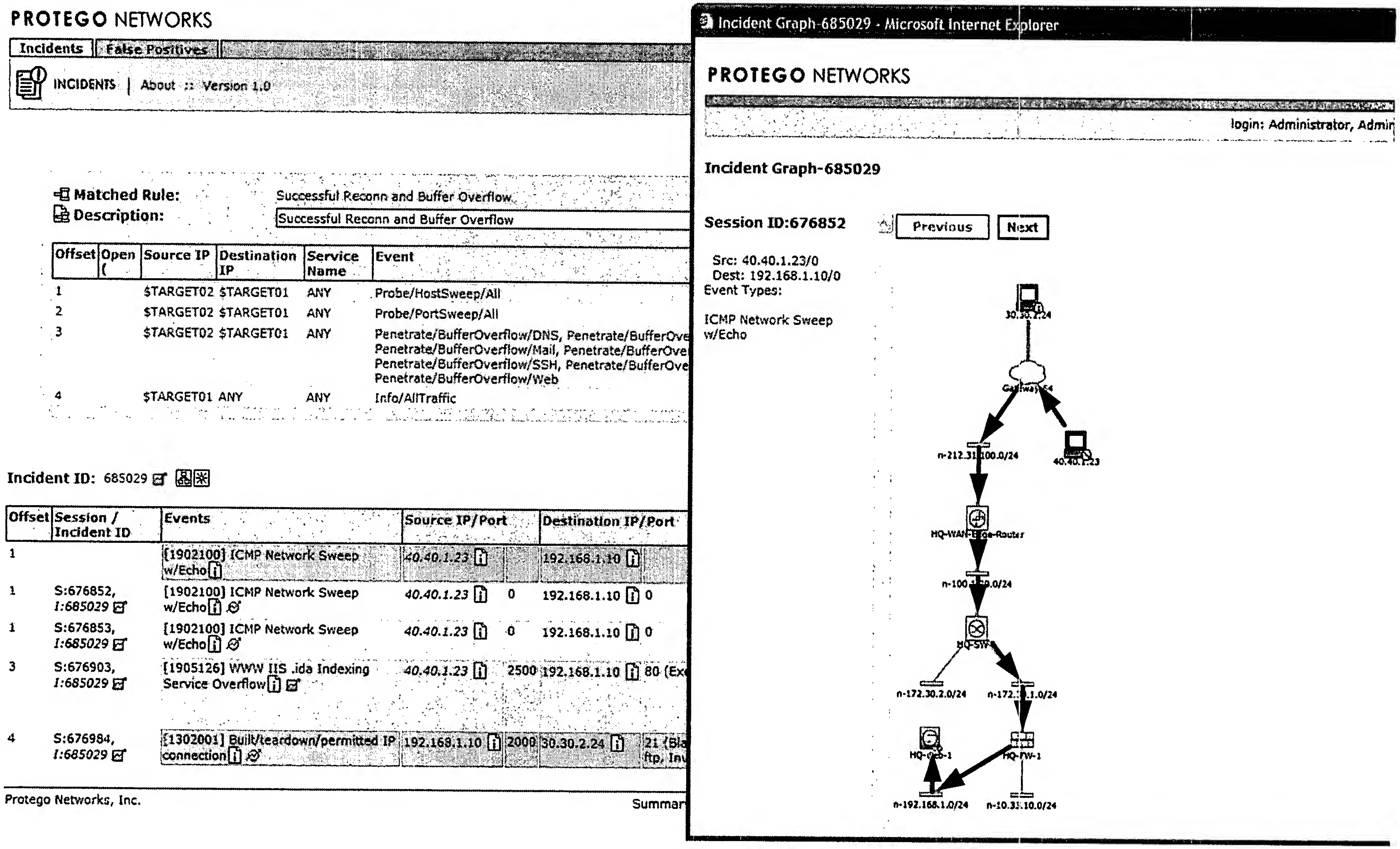
Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23	192.168.1.10		⊟ Total: 2					
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23 0	192.168.1.10 0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23 0	192.168.1.10 0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23 2500	192.168.1.10 80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10 2000	30.30.2.24 21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 11(A)



PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Version 1.0

Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOve Penetrate/BufferOverflow/Mail, Penetrate/BufferOve Penetrate/BufferOverflow/SSH, Penetrate/BufferOve Penetrate/BufferOverflow/Web
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port	
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10	
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Ex
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (Bla ftp, Inv

Protego Networks, Inc.

Summar

Incident Graph-685029 - Microsoft Internet Explorer

PROTEGO NETWORKS

login: Administrator, Admin

Incident Graph-685029

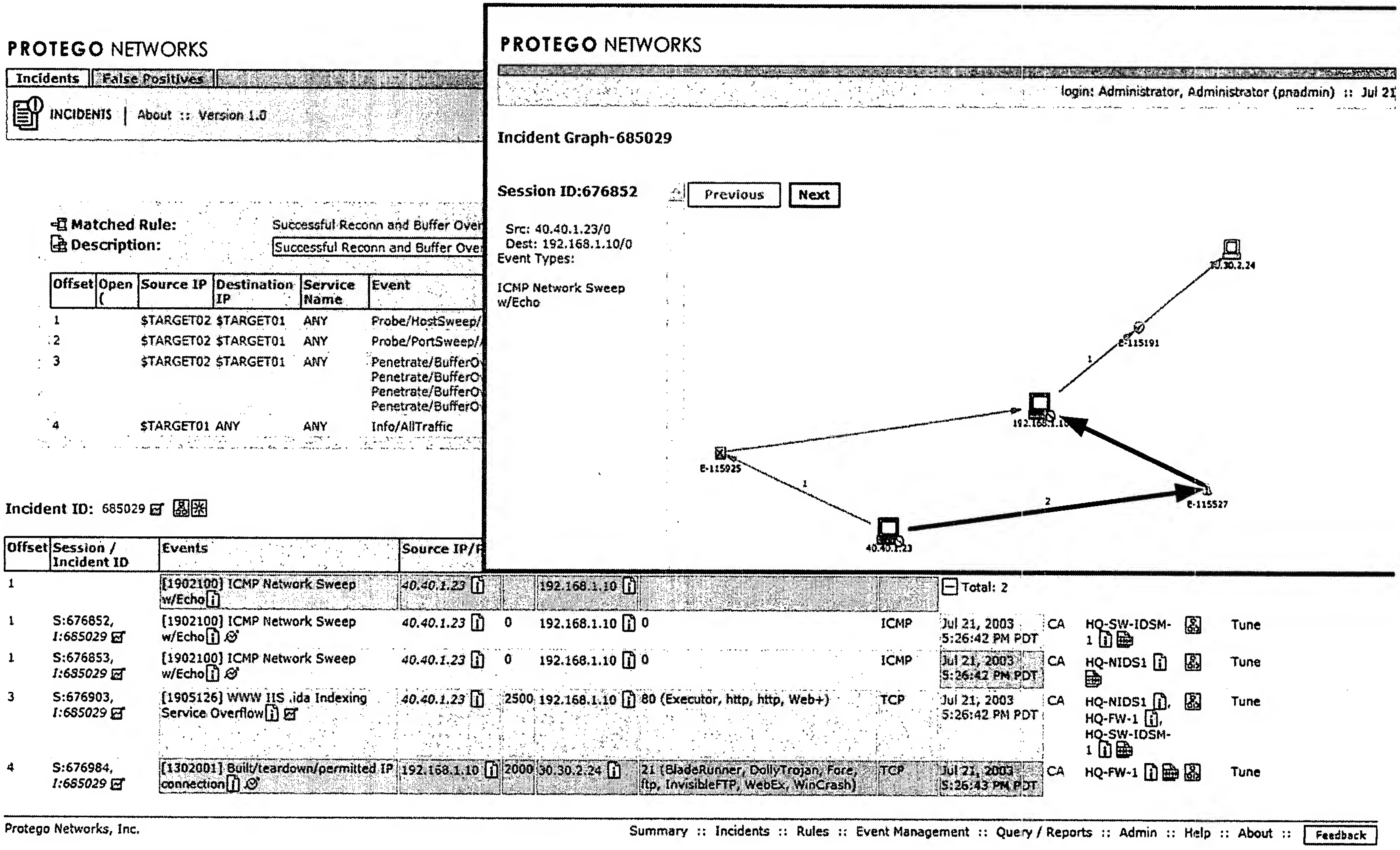
Session ID:676852

Previous | Next

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep w/Echo

Fig. 11(B)



PROTEGO NETWORKS

Matched Rule: Successful Reconn and Buffer Over

Description: Successful Reconn and Buffer Ove

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/P									
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			⊟ Total: 2				
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 21

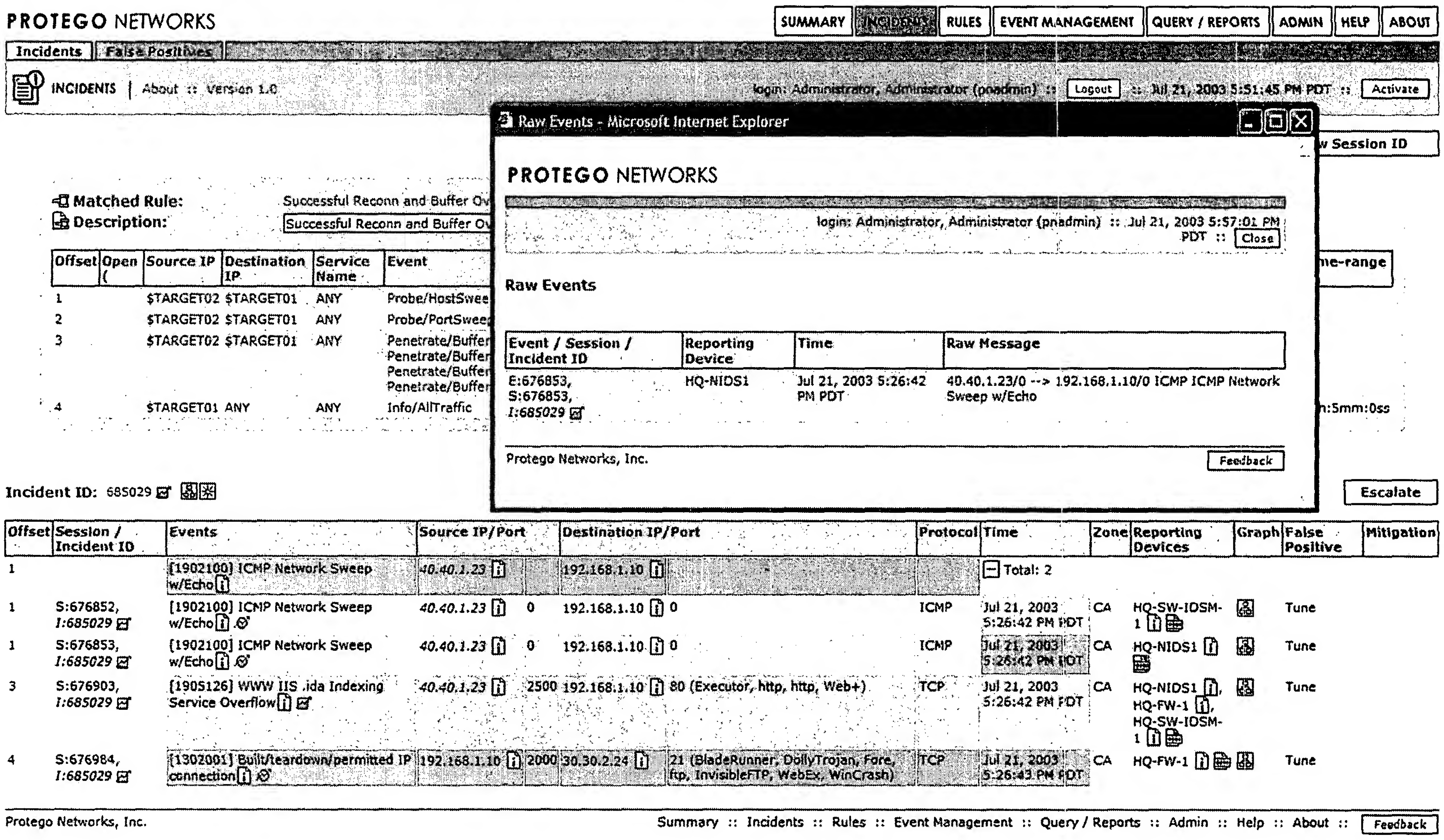
Incident Graph-685029

Session ID:676852

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep w/Echo

Fig. 11(C)



PROTEGO NETWORKS

SUMMARY | INCIDENTS | RULES | EVENT MANAGEMENT | QUERY / REPORTS | ADMIN | HELP | ABOUT

Incidents | False Positives

INCIDENTS | About :: Version 1.0

login: Administrator, Administrator (pnadmin) :: Logout :: Jul 21, 2003 5:51:45 PM PDT :: Activate

Matched Rule: Successful Reconn and Buffer Ov

Description: Successful Reconn and Buffer Ov

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSwee
2		$TARGET02	$TARGET01	ANY	Probe/PortSwee
3		$TARGET02	$TARGET01	ANY	Penetrate/Buffer Penetrate/Buffer Penetrate/Buffer Penetrate/Buffer
4		$TARGET01	ANY	ANY	Info/AllTraffic

w Session ID

ne-range

h:5mm:0ss

Raw Events - Microsoft Internet Explorer

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 21, 2003 5:57:01 PM PDT :: Close

Raw Events

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:676853, S:676853, I:685029	HQ-NIDS1	Jul 21, 2003 5:26:42 PM PDT	40.40.1.23/0 --> 192.168.1.10/0 ICMP ICMP Network Sweep w/Echo

Protego Networks, Inc.

Feedback

Incident ID: 685029

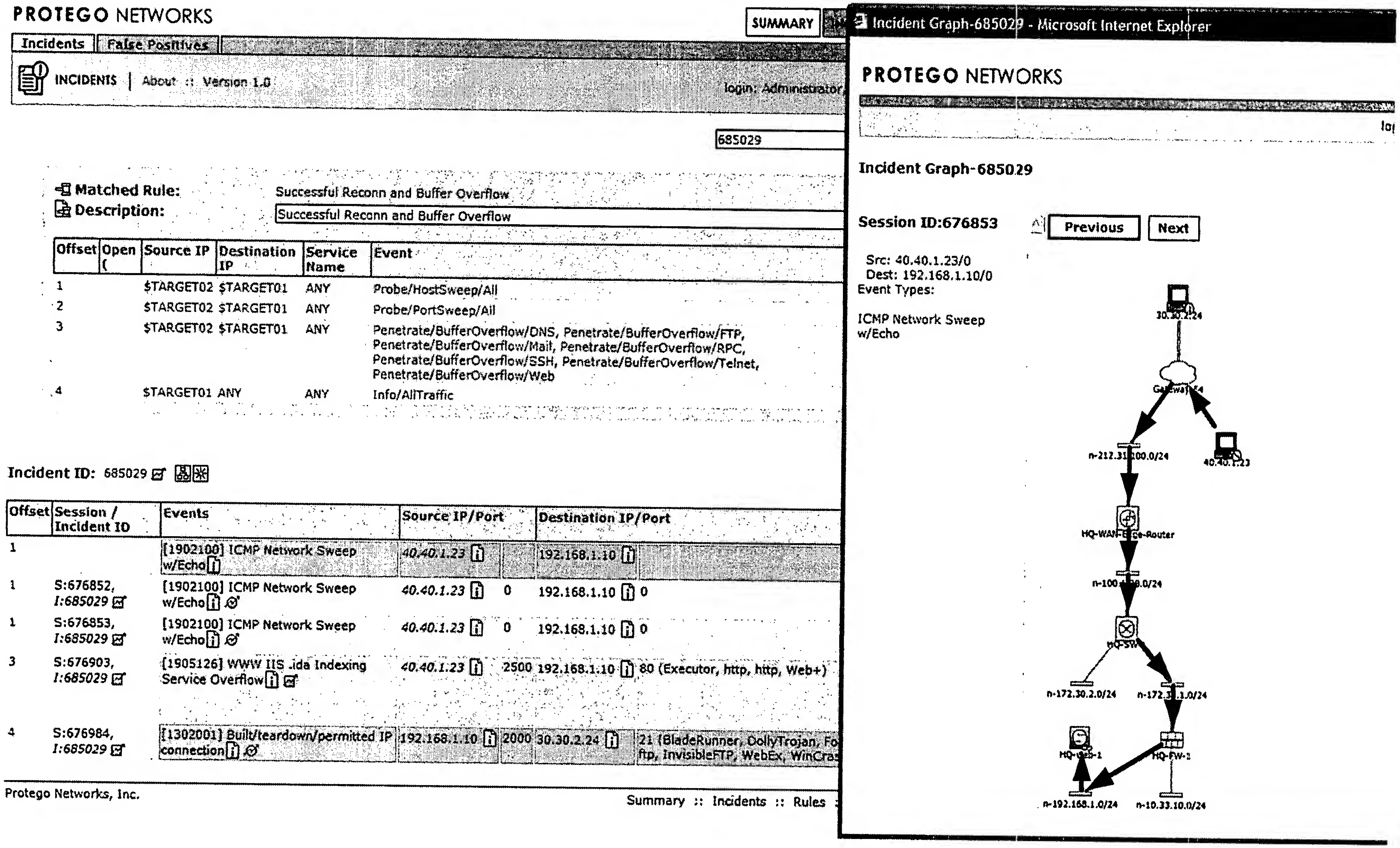
Escalate

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			⊟ Total: 2					
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 12(A)



PROTEGO NETWORKS

685029

Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10 0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10 0
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10 80 (Executor, http, http, Web+)
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24 21 (BladeRunner, DollyTrojan, Fo ftp, InvisibleFTP, WebEx, WinCra

Protego Networks, Inc.

Incident Graph-685029 - Microsoft Internet Explorer

PROTEGO NETWORKS

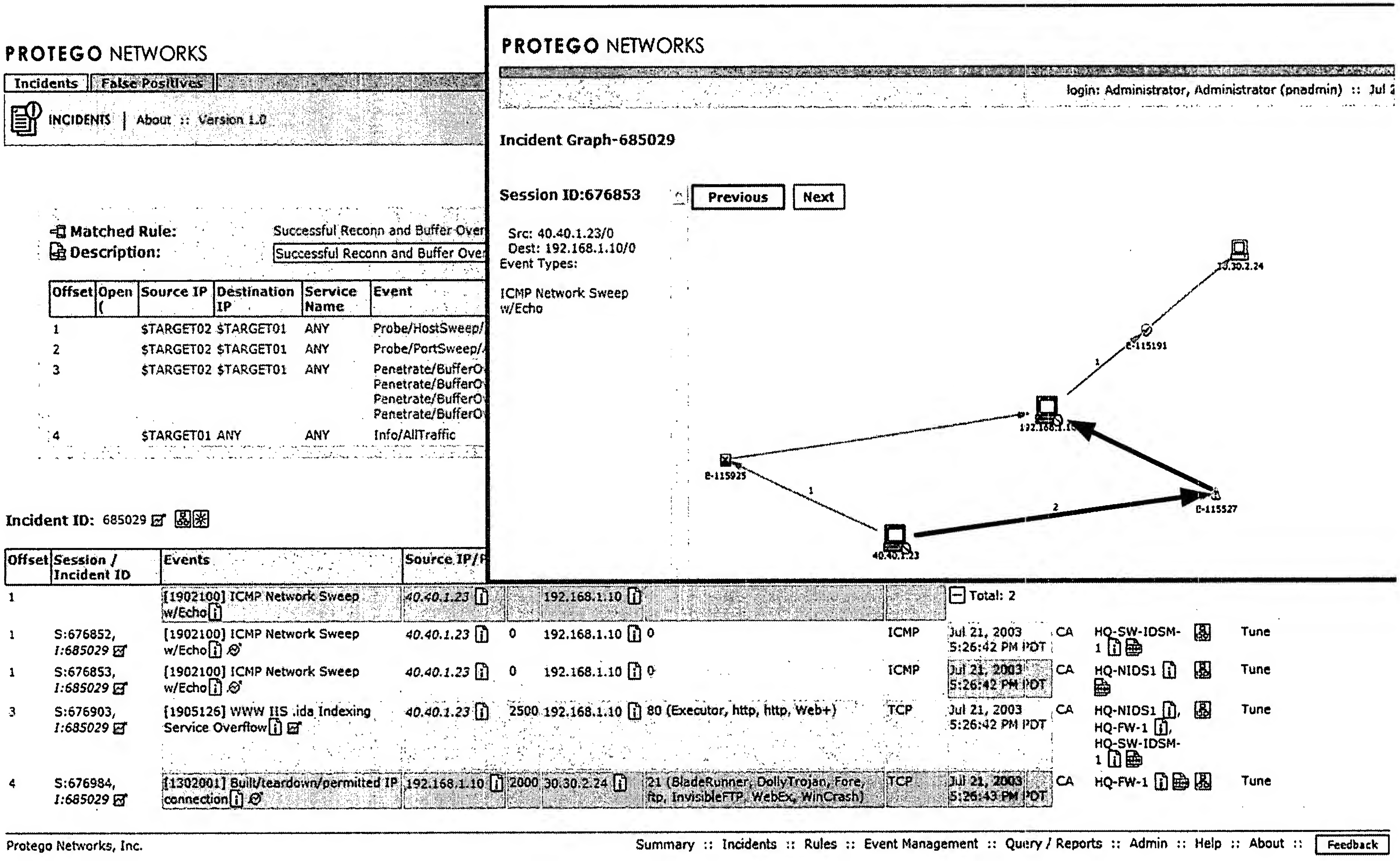
Incident Graph-685029

Session ID:676853

Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep w/Echo

Fig. 12(B)



PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Version 1.0

Matched Rule: Successful Reconn and Buffer Over

Description: Successful Reconn and Buffer Over

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/P									
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10				⊟ Total: 2			
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 2

Incident Graph-685029

Session ID:676853 Previous Next

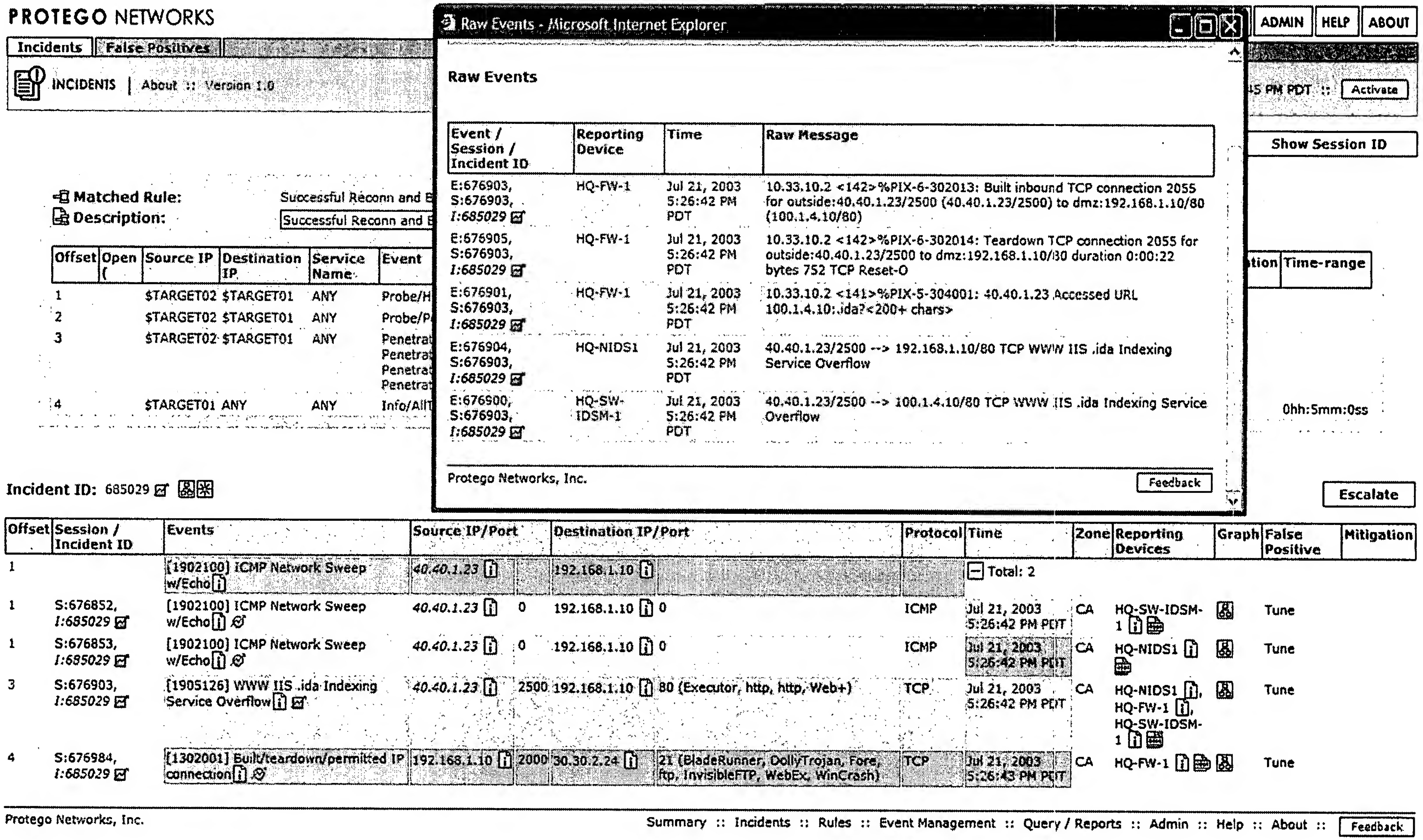
Src: 40.40.1.23/0
Dest: 192.168.1.10/0
Event Types:

ICMP Network Sweep w/Echo

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 12(C)



Matched Rule: Successful Reconn and E

Description: Successful Reconn and E

Offset	Open (	Source IP	Destination IP	Service Name	Event	tion	Time-range
1		$TARGET02	$TARGET01	ANY	Probe/H		
2		$TARGET02	$TARGET01	ANY	Probe/P		
3		$TARGET02	$TARGET01	ANY	Penetrat Penetrat Penetrat Penetrat		
4		$TARGET01	ANY	ANY	Info/AllT		0hh:5mm:0ss

Raw Events

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:676903, S:676903, I:685029	HQ-FW-1	Jul 21, 2003 5:26:42 PM PDT	10.33.10.2 <142>%PIX-6-302013: Built inbound TCP connection 2055 for outside:40.40.1.23/2500 (40.40.1.23/2500) to dmz:192.168.1.10/80 (100.1.4.10/80)
E:676905, S:676903, I:685029	HQ-FW-1	Jul 21, 2003 5:26:42 PM PDT	10.33.10.2 <142>%PIX-6-302014: Teardown TCP connection 2055 for outside:40.40.1.23/2500 to dmz:192.168.1.10/80 duration 0:00:22 bytes 752 TCP Reset-O
E:676901, S:676903, I:685029	HQ-FW-1	Jul 21, 2003 5:26:42 PM PDT	10.33.10.2 <141>%PIX-5-304001: 40.40.1.23 Accessed URL 100.1.4.10:.ida?<200+ chars>
E:676904, S:676903, I:685029	HQ-NIDS1	Jul 21, 2003 5:26:42 PM PDT	40.40.1.23/2500 --> 192.168.1.10/80 TCP WWW IIS .ida Indexing Service Overflow
E:676900, S:676903, I:685029	HQ-SW-IDSM-1	Jul 21, 2003 5:26:42 PM PDT	40.40.1.23/2500 --> 100.1.4.10/80 TCP WWW IIS .ida Indexing Service Overflow

Protego Networks, Inc.

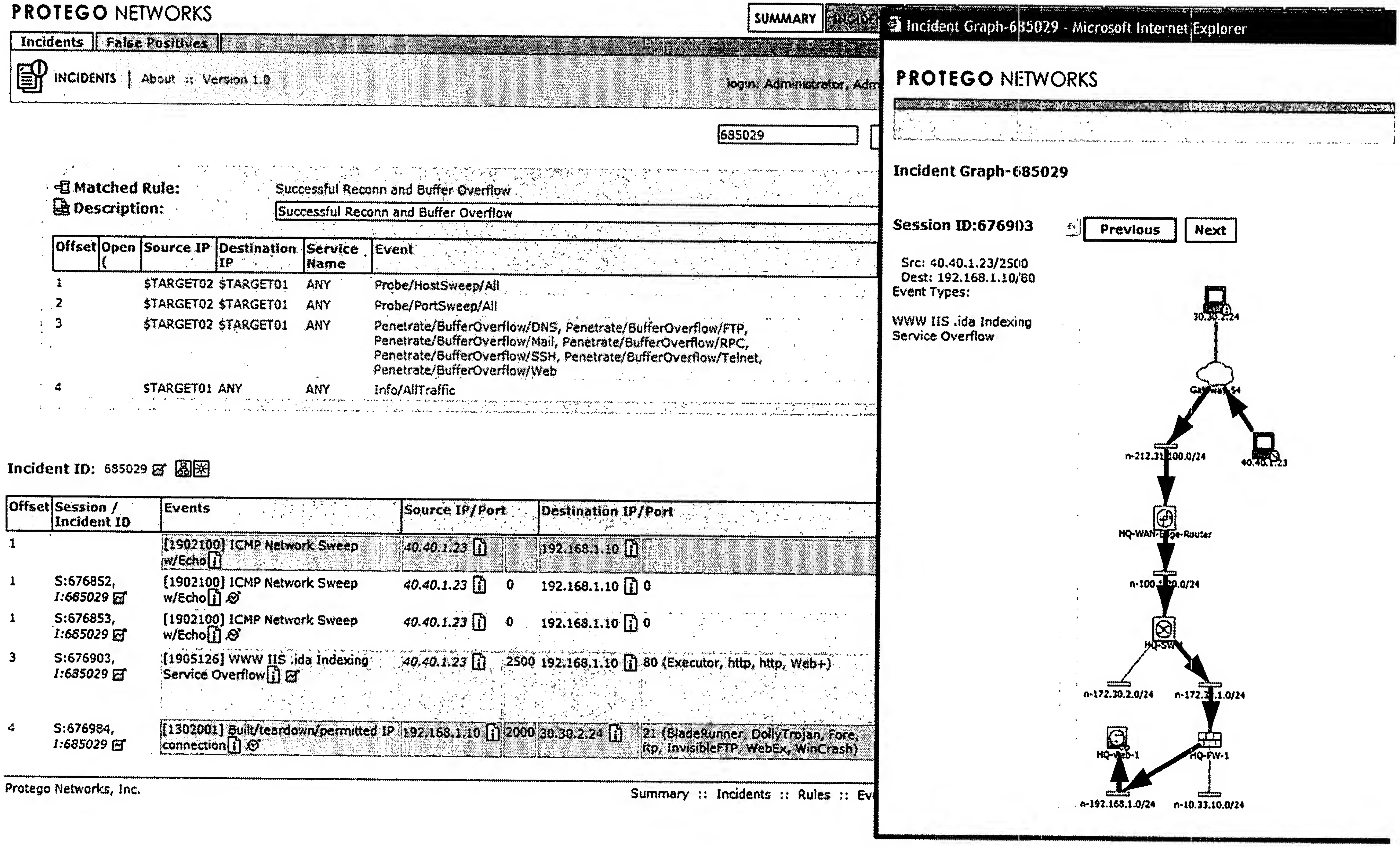
Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			Total: 2					
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::
Feedback

Fig. 13(A)



Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port	
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10	
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)

Protego Networks, Inc.

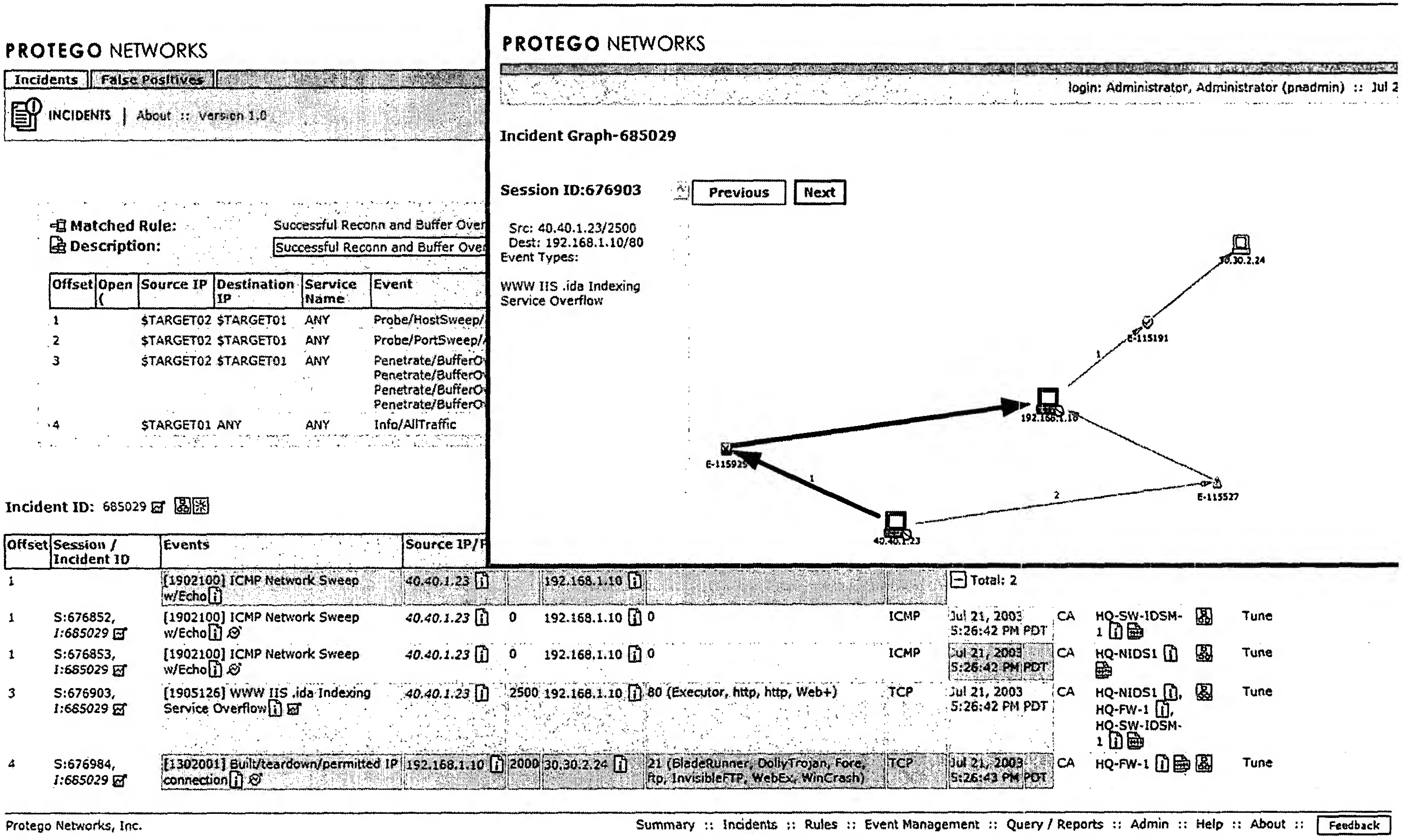
Incident Graph-685029

Session ID:676903

Src: 40.40.1.23/2500
Dest: 192.168.1.10/80
Event Types:

WWW IIS .ida Indexing Service Overflow

Fig. 13(B)



PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Version 1.0

Matched Rule: Successful Reconn and Buffer Over

Description: Successful Reconn and Buffer Ove

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/P									
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			⊟ Total: 2				
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 2

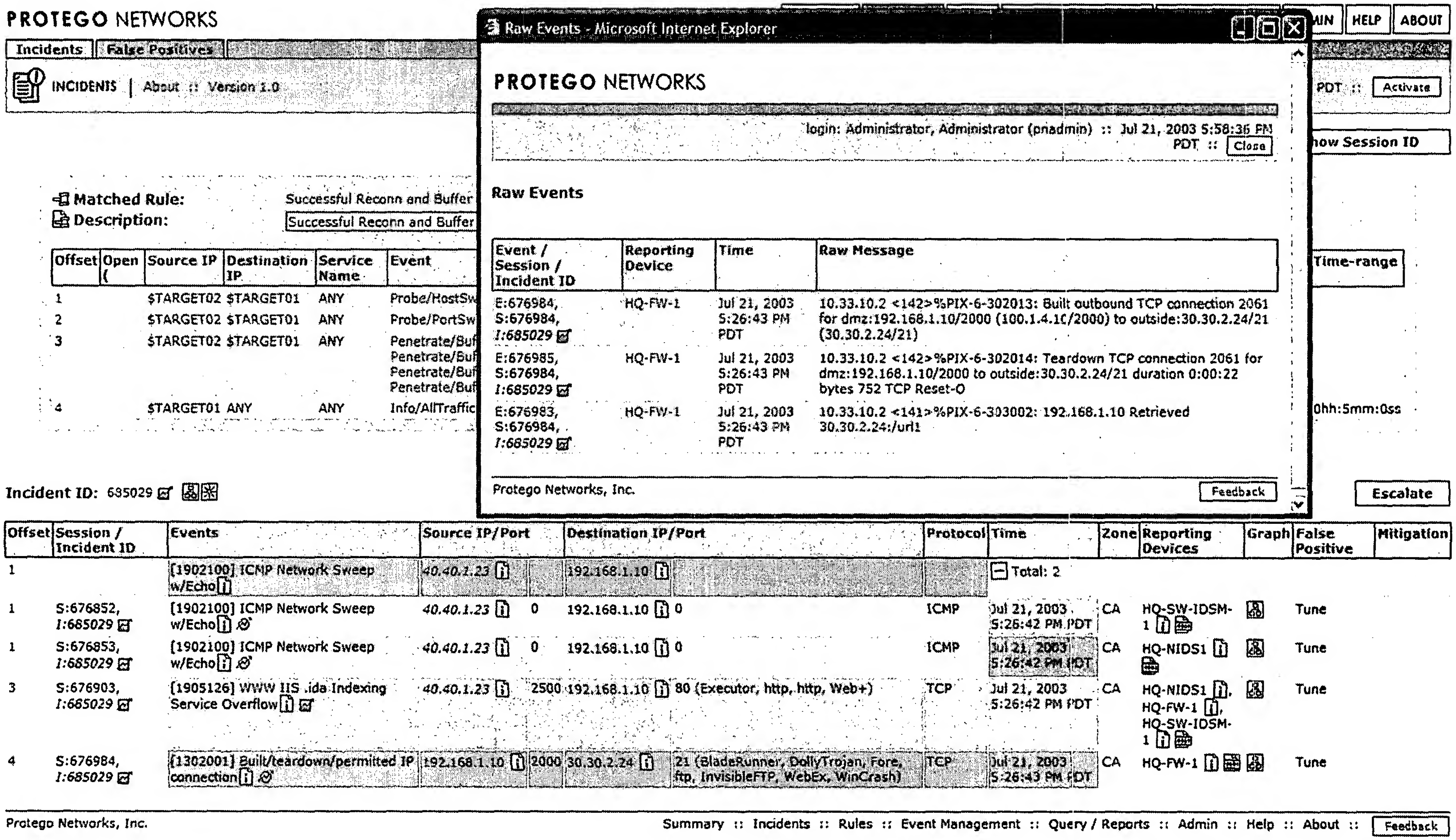
Incident Graph-685029

Session ID:676903 Previous Next

Src: 40.40.1.23/2500
Dest: 192.168.1.10/80
Event Types:

WWW IIS .ida Indexing
Service Overflow

Fig. 13(C)



PROTEGO NETWORKS

Matched Rule: Successful Reconn and Buffer

Description: Successful Reconn and Buffer

Offset	Open (	Source IP	Destination IP	Service Name	Event	Time-range
1		$TARGET02	$TARGET01	ANY	Probe/HostSw	
2		$TARGET02	$TARGET01	ANY	Probe/PortSw	
3		$TARGET02	$TARGET01	ANY	Penetrate/Buf Penetrate/Buf Penetrate/Buf Penetrate/Buf	
4		$TARGET01	ANY	ANY	Info/AllTraffic	0hh:5mm:0ss

Raw Events - Microsoft Internet Explorer

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 21, 2003 5:58:36 PM PDT :: Close

Raw Events

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:676984, S:676984, I:685029	HQ-FW-1	Jul 21, 2003 5:26:43 PM PDT	10.33.10.2 <142>%PIX-6-302013: Built outbound TCP connection 2061 for dmz:192.168.1.10/2000 (100.1.4.1C/2000) to outside:30.30.2.24/21 (30.30.2.24/21)
E:676985, S:676984, I:685029	HQ-FW-1	Jul 21, 2003 5:26:43 PM PDT	10.33.10.2 <142>%PIX-6-302014: Teardown TCP connection 2061 for dmz:192.168.1.10/2000 to outside:30.30.2.24/21 duration 0:00:22 bytes 752 TCP Reset-O
E:676983, S:676984, I:685029	HQ-FW-1	Jul 21, 2003 5:26:43 PM PDT	10.33.10.2 <141>%PIX-6-303002: 192.168.1.10 Retrieved 30.30.2.24:/url1

Protego Networks, Inc.

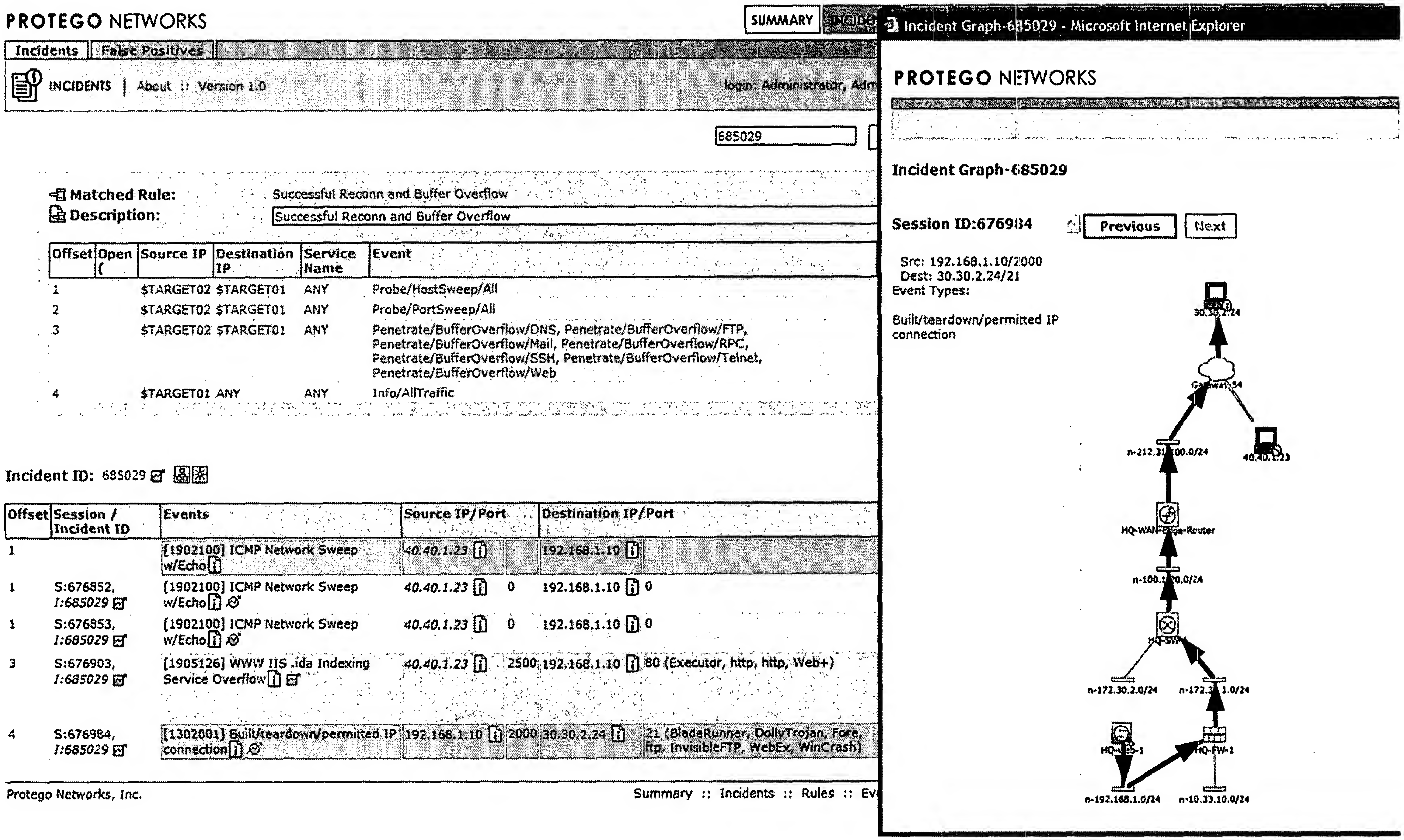
Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			⊟ Total: 2					
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune	
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune	
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune	
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::
Feedback

Fig. 14(A)



PROTEGO NETWORKS

SUMMARY

Incidents | False Positives

INCIDENTS | About :: Version 1.0

login: Administrator, Adm

685029

Matched Rule: Successful Reconn and Buffer Overflow

Description: Successful Reconn and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/All
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/All
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/SSH, Penetrate/BufferOverflow/Telnet, Penetrate/BufferOverflow/Web
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port	
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10	
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Ev

Incident Graph-685029 - Microsoft Internet Explorer

PROTEGO NETWORKS

Incident Graph-685029

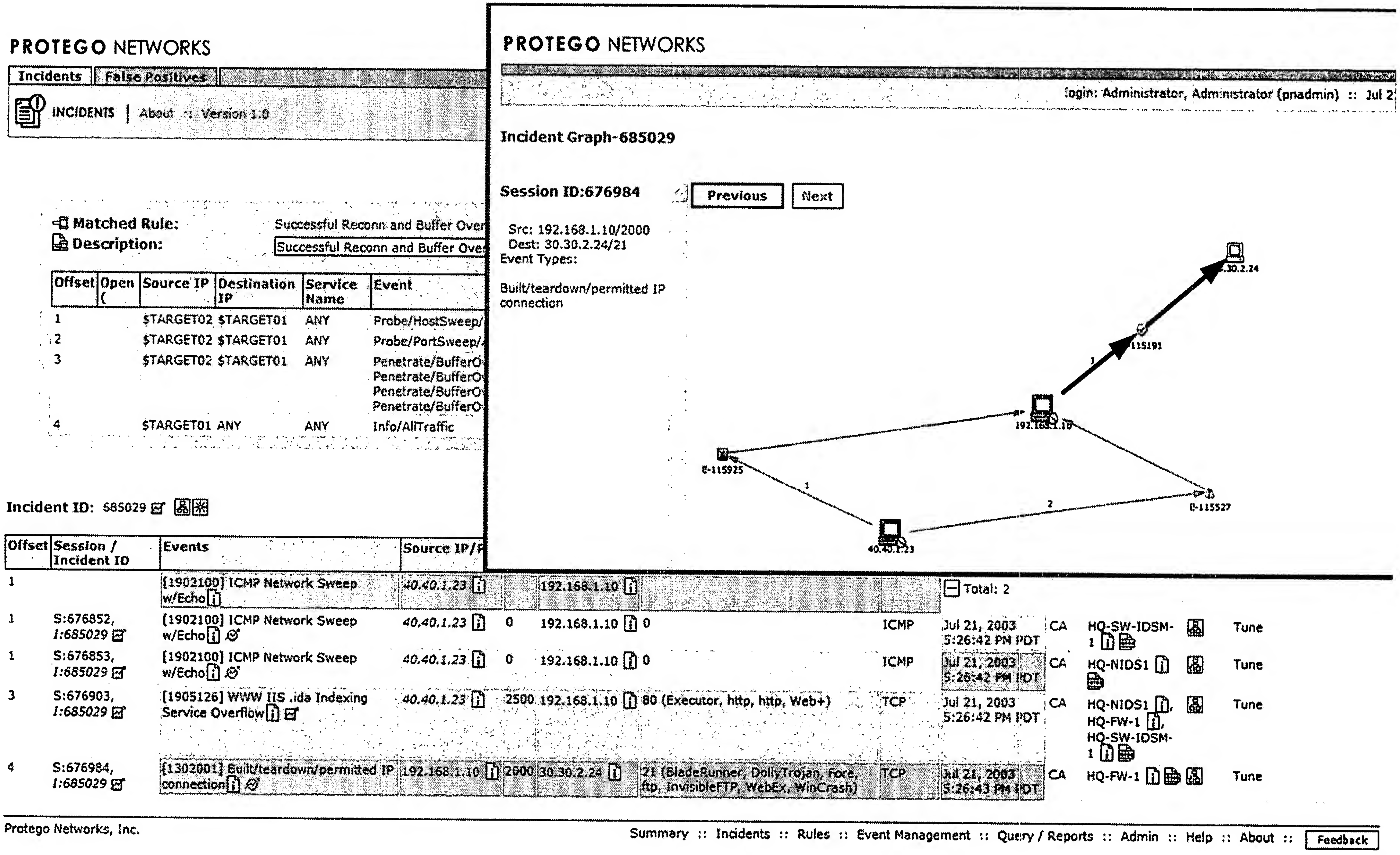
Session ID:676984

Previous Next

Src: 192.168.1.10/2000
Dest: 30.30.2.24/21
Event Types:

Built/teardown/permitted IP connection

Fig. 14(B)



PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Version 1.0

Matched Rule: Successful Reconn and Buffer Over

Description: Successful Reconn and Buffer Ove

Offset	Open (	Source IP	Destination IP	Service Name	Event
1		$TARGET02	$TARGET01	ANY	Probe/HostSweep/
2		$TARGET02	$TARGET01	ANY	Probe/PortSweep/
3		$TARGET02	$TARGET01	ANY	Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO Penetrate/BufferO
4		$TARGET01	ANY	ANY	Info/AllTraffic

Incident ID: 685029

Offset	Session / Incident ID	Events	Source IP/P									
1		[1902100] ICMP Network Sweep w/Echo	40.40.1.23		192.168.1.10			⊟ Total: 2				
1	S:676852, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-SW-IDSM-1		Tune
1	S:676853, I:685029	[1902100] ICMP Network Sweep w/Echo	40.40.1.23	0	192.168.1.10	0	ICMP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1		Tune
3	S:676903, I:685029	[1905126] WWW IIS .ida Indexing Service Overflow	40.40.1.23	2500	192.168.1.10	80 (Executor, http, http, Web+)	TCP	Jul 21, 2003 5:26:42 PM PDT	CA	HQ-NIDS1, HQ-FW-1, HQ-SW-IDSM-1		Tune
4	S:676984, I:685029	[1302001] Built/teardown/permitted IP connection	192.168.1.10	2000	30.30.2.24	21 (BladeRunner, DollyTrojan, Fore, ftp, InvisibleFTP, WebEx, WinCrash)	TCP	Jul 21, 2003 5:26:43 PM PDT	CA	HQ-FW-1		Tune

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 2

Incident Graph-685029

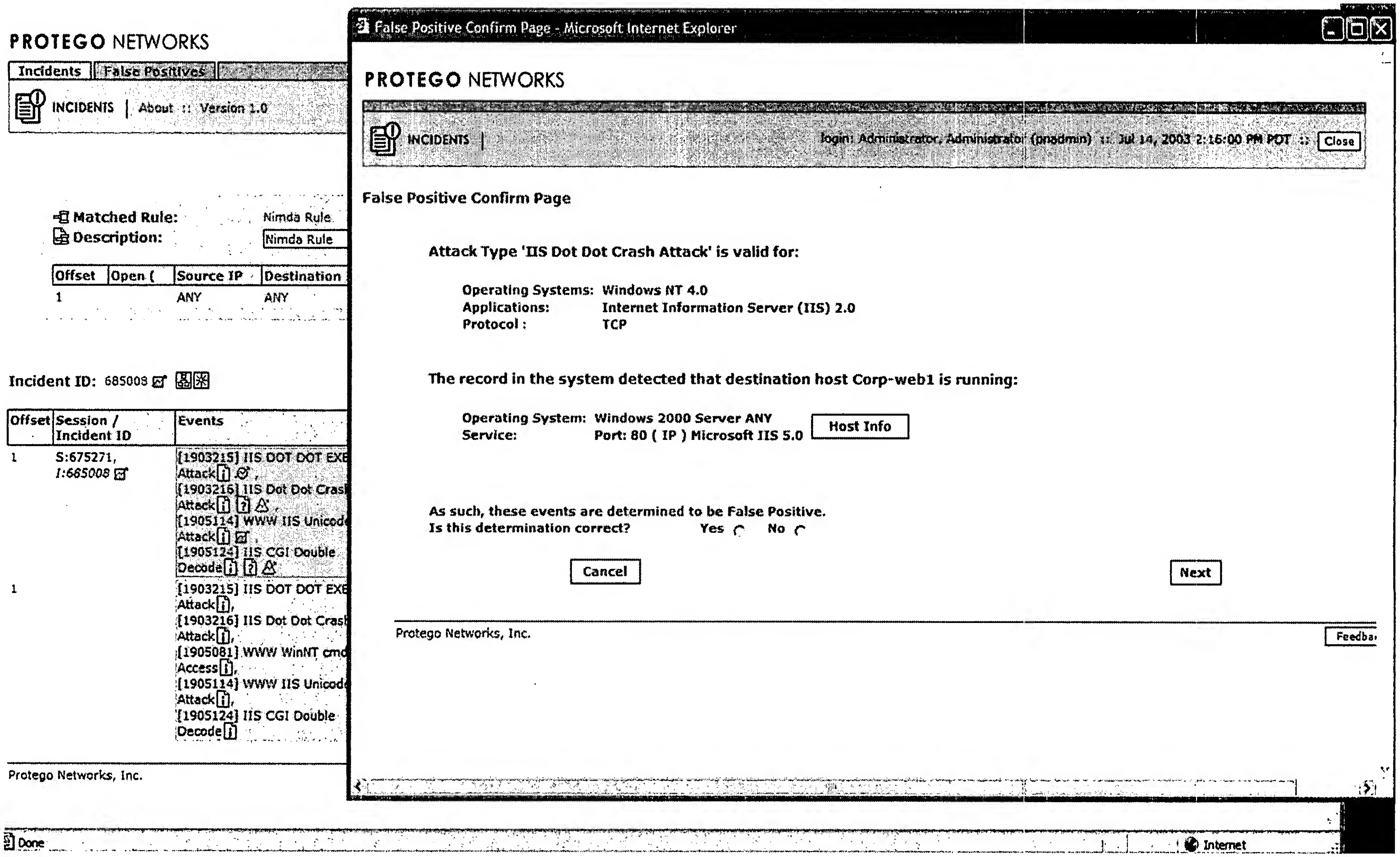
Session ID:676984

Previous | Next

Src: 192.168.1.10/2000
Dest: 30.30.2.24/21
Event Types:

Built/teardown/permitted IP connection

Fig. 14(C)



PROTEGO NETWORKS

Matched Rule: Nimda Rule
Description: Nimda Rule

Offset	Open (	Source IP	Destination
1		ANY	ANY

Incident ID: 685008

Offset	Session / Incident ID	Events
1	S:675271, I:685008	[1903215] IIS DOT DOT EXE Attack , [1903216] IIS Dot Dot Crasl Attack , [1905114] WWW IIS Unicode Attack , [1905124] IIS CGI Double Decode
1		[1903215] IIS DOT DOT EXE Attack, [1903216] IIS Dot Dot Crasl Attack, [1905081] WWW WinNT cmd Access, [1905114] WWW IIS Unicode Attack, [1905124] IIS CGI Double Decode

Protego Networks, Inc.

False Positive Confirm Page - Microsoft Internet Explorer

PROTEGO NETWORKS

login: Administrator, Administrator (pnadmin) :: Jul 14, 2003 2:16:00 PM PDT ::

False Positive Confirm Page

Attack Type 'IIS Dot Dot Crash Attack' is valid for:

Operating Systems: Windows NT 4.0
Applications: Internet Information Server (IIS) 2.0
Protocol : TCP

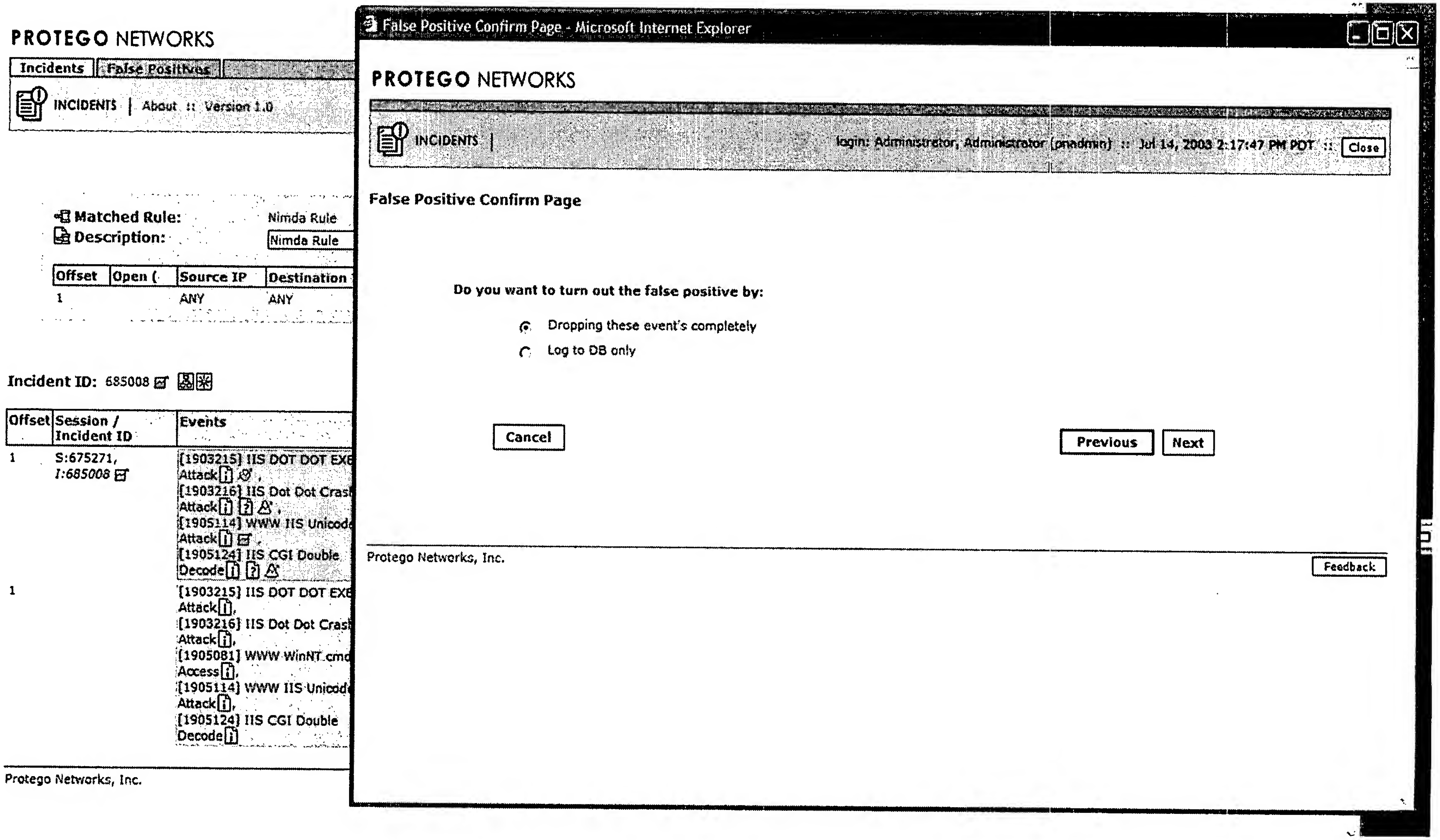
The record in the system detected that destination host Corp-web1 is running:

Operating System: Windows 2000 Server ANY
Service: Port: 80 (IP) Microsoft IIS 5.0

As such, these events are determined to be False Positive.
Is this determination correct? Yes ○ No ○

Protego Networks, Inc.

Fig. 15(A)



PROTEGO NETWORKS

Incidents | False Positives

INCIDENTS | About :: Version 1.0

Matched Rule: Nimda Rule

Description: Nimda Rule

Offset	Open (	Source IP	Destination
1		ANY	ANY

Incident ID: 685008

Offset	Session / Incident ID	Events
1	S:675271, I:685008	[1903215] IIS DOT DOT EXE Attack, [1903216] IIS Dot Dot Crash Attack, [1905114] WWW IIS Unicode Attack, [1905124] IIS CGI Double Decode
1		[1903215] IIS DOT DOT EXE Attack, [1903216] IIS Dot Dot Crash Attack, [1905081] WWW WinNT cmd Access, [1905114] WWW IIS Unicode Attack, [1905124] IIS CGI Double Decode

Protego Networks, Inc.

False Positive Confirm Page - Microsoft Internet Explorer

PROTEGO NETWORKS

INCIDENTS | login: Administrator, Administrator (pnadmin) :: Jul 14, 2003 2:17:47 PM PDT :: Close

False Positive Confirm Page

Do you want to turn out the false positive by:

● Dropping these event's completely

○ Log to DB only

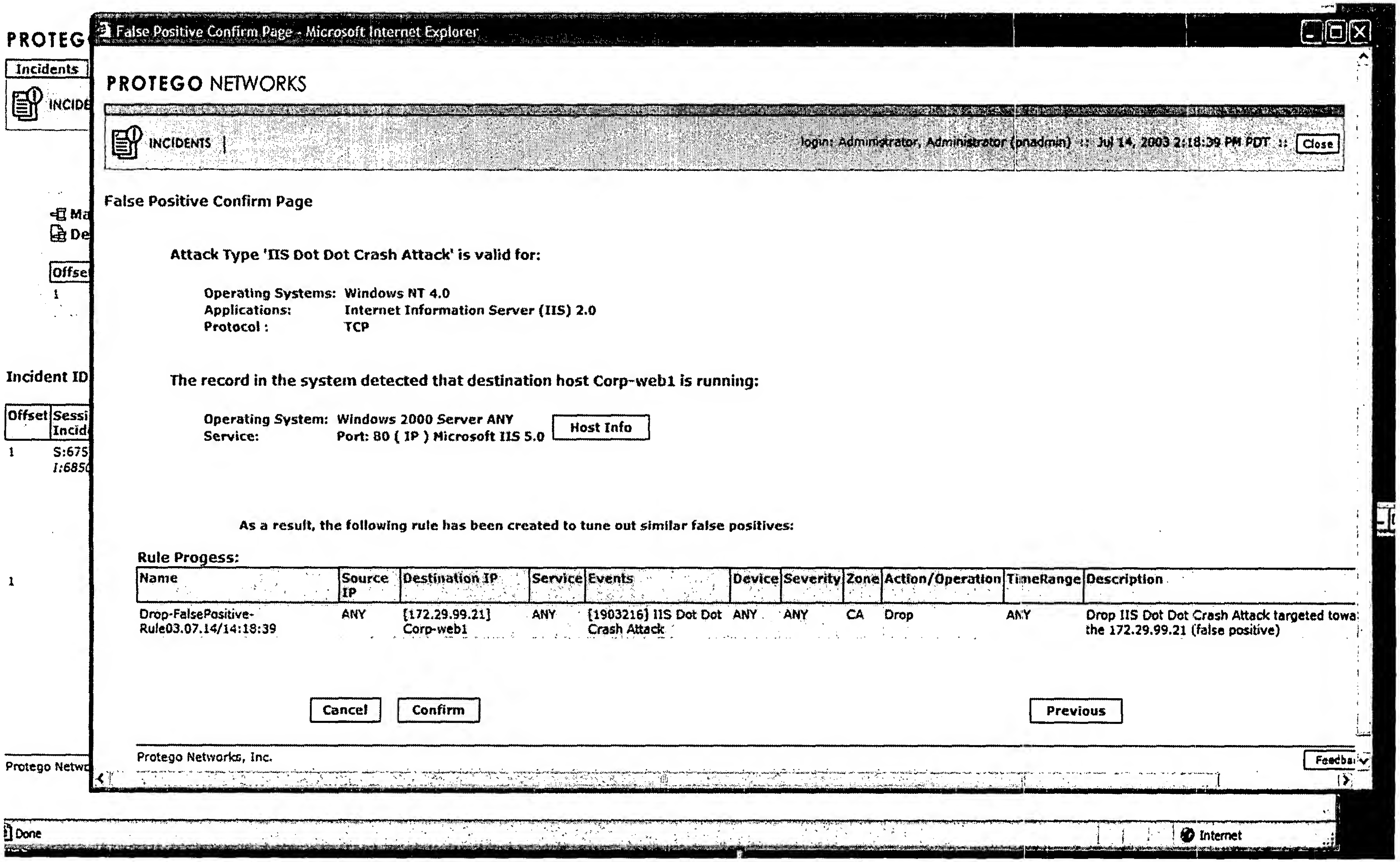
Cancel

Previous Next

Protego Networks, Inc.

Feedback

Fig. 15(B)



login: Administrator, Administrator (pnadmin) :: Jul 14, 2003 2:18:39 PM PDT ::

False Positive Confirm Page

Attack Type 'IIS Dot Dot Crash Attack' is valid for:

Operating Systems: Windows NT 4.0
Applications: Internet Information Server (IIS) 2.0
Protocol : TCP

The record in the system detected that destination host Corp-web1 is running:

Operating System: Windows 2000 Server ANY
Service: Port: 80 (IP) Microsoft IIS 5.0

Host Info

As a result, the following rule has been created to tune out similar false positives:

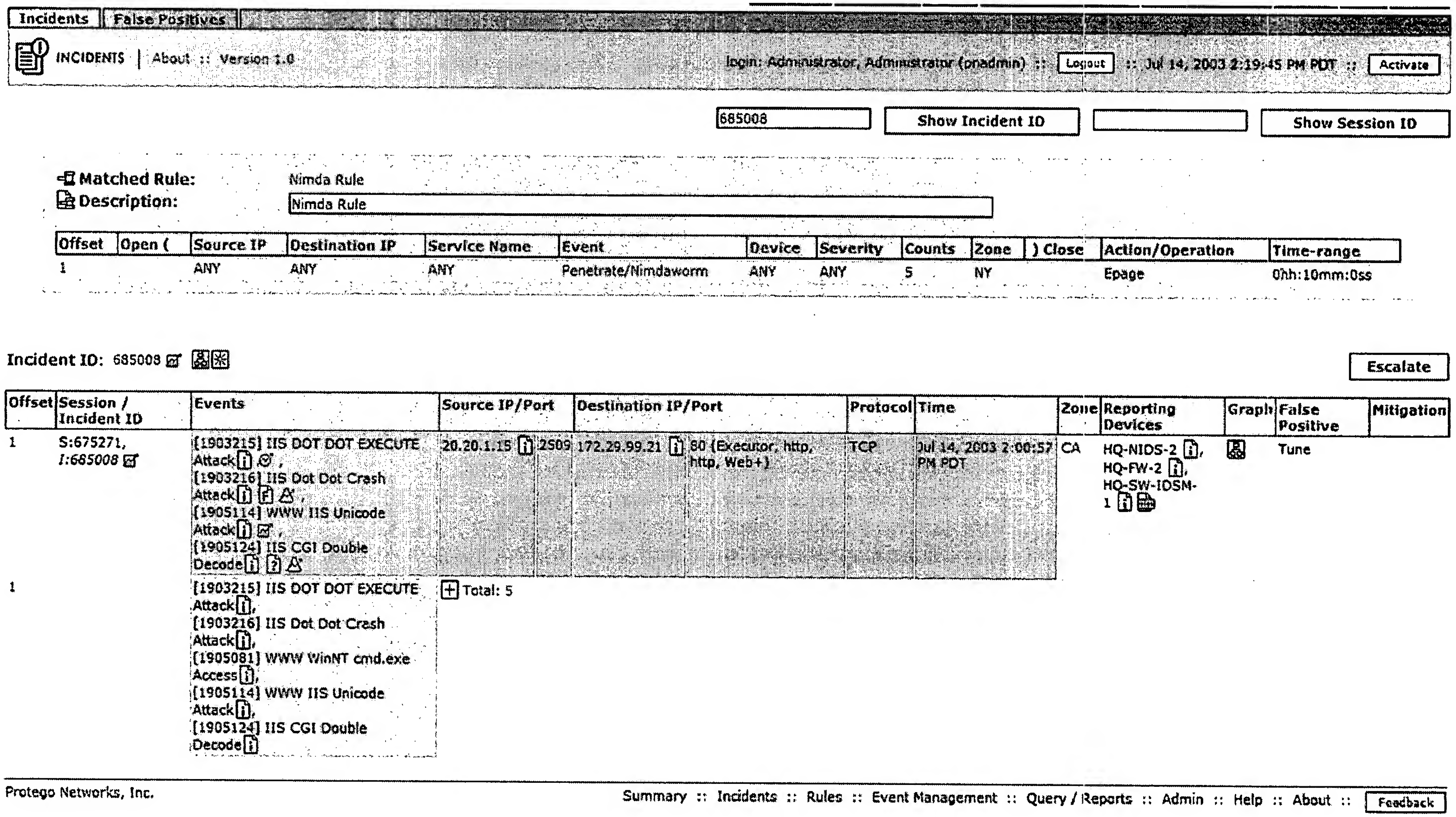
Rule Progess:

Name	Source IP	Destination IP	Service	Events	Device	Severity	Zone	Action/Operation	TimeRange	Description
Drop-FalsePositive-Rule03.07.14/14:18:39	ANY	[172.29.99.21] Corp-web1	ANY	[1903216] IIS Dot Dot Crash Attack	ANY	ANY	CA	Drop	ANY	Drop IIS Dot Dot Crash Attack targeted towa the 172.29.99.21 (false positive)

Cancel Confirm Previous

Protego Networks, Inc.

Fig. 15(C)



Incidents
False Positives
INCIDENTS | About :: Version 1.0
login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14, 2003 2:19:45 PM PDT :: Activate
685008
Show Incident ID
Show Session ID

Matched Rule: Nimda Rule

Description: Nimda Rule

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
1		ANY	ANY	ANY	Penetrate/Nimdaworm	ANY	ANY	5	NY		Epage	0hh:10mm:0ss

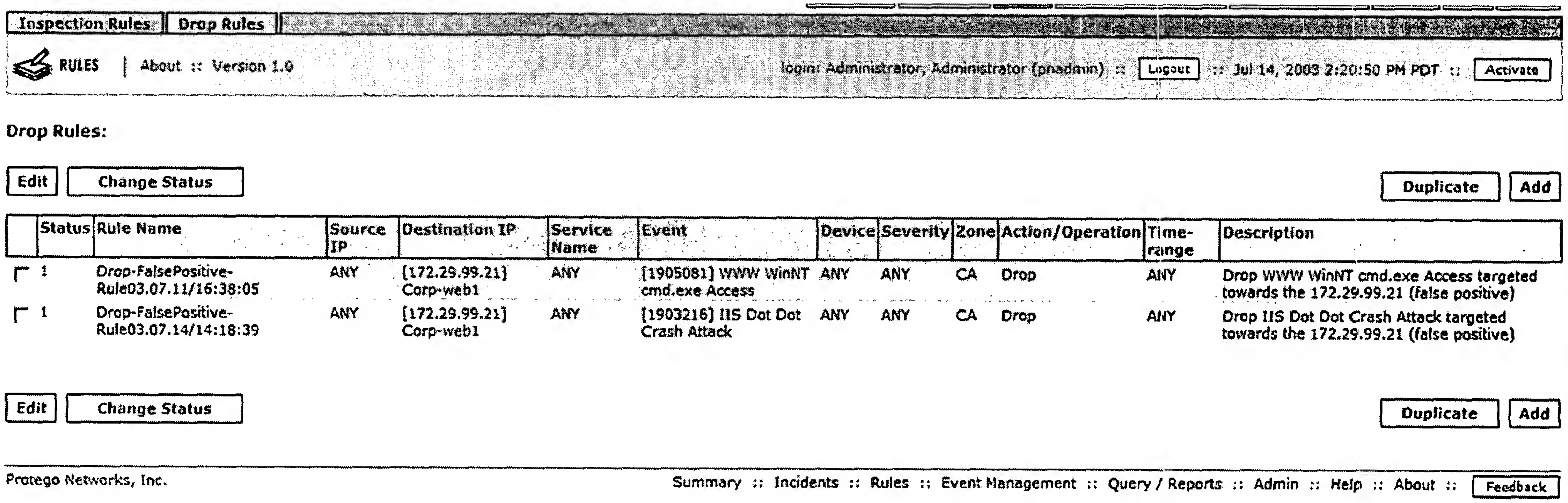
Incident ID: 685008

Offset	Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1	S:675271, I:685008	[1903215] IIS DOT DOT EXECUTE Attack ⓘ, [1903216] IIS Dot Dot Crash Attack ⓘ, [1905114] WWW IIS Unicode Attack ⓘ, [1905124] IIS CGI Double Decode ⓘ	20.20.1.15 ⓘ 2509	172.29.99.21 ⓘ 80 (Executor, http, http, Web+)	TCP	Jul 14, 2003 2:00:57 PM PDT	CA	HQ-NIDS-2 ⓘ, HQ-FW-2 ⓘ, HQ-SW-IDSM-1 ⓘ		Tune	
1		[1903215] IIS DOT DOT EXECUTE Attack ⓘ, [1903216] IIS Dot Dot Crash Attack ⓘ, [1905081] WWW WinNT cmd.exe Access ⓘ, [1905114] WWW IIS Unicode Attack ⓘ, [1905124] IIS CGI Double Decode ⓘ	⊞ Total: 5								

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 15(D)


Inspection Rules
Drop Rules
RULES | About :: Version 1.0
login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14, 2003 2:20:50 PM PDT :: Activate

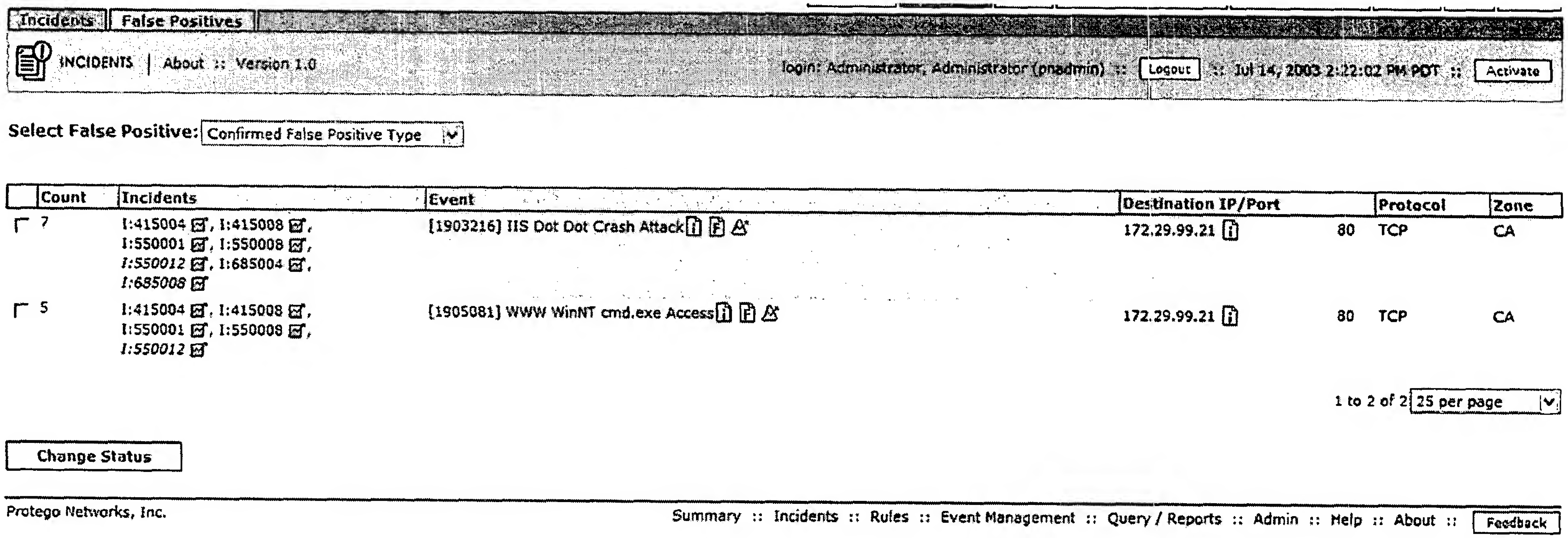
Drop Rules:

Edit
Change Status
Duplicate
Add

	Status	Rule Name	Source IP	Destination IP	Service Name	Event	Device	Severity	Zone	Action/Operation	Time-range	Description
☐	1	Drop-FalsePositive-Rule03.07.11/16:38:05	ANY	[172.29.99.21] Corp-web1	ANY	[1905081] WWW WinNT cmd.exe Access	ANY	ANY	CA	Drop	ANY	Drop WWW WinNT cmd.exe Access targeted towards the 172.29.99.21 (false positive)
☐	1	Drop-FalsePositive-Rule03.07.14/14:18:39	ANY	[172.29.99.21] Corp-web1	ANY	[1903216] IIS Dot Dot Crash Attack	ANY	ANY	CA	Drop	ANY	Drop IIS Dot Dot Crash Attack targeted towards the 172.29.99.21 (false positive)

Edit
Change Status
Duplicate
Add
Protego Networks, Inc.
Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 16(A)



Incidents
False Positives
INCIDENTS | About :: Version 1.0
login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14, 2003 2:22:02 PM PDT :: Activate

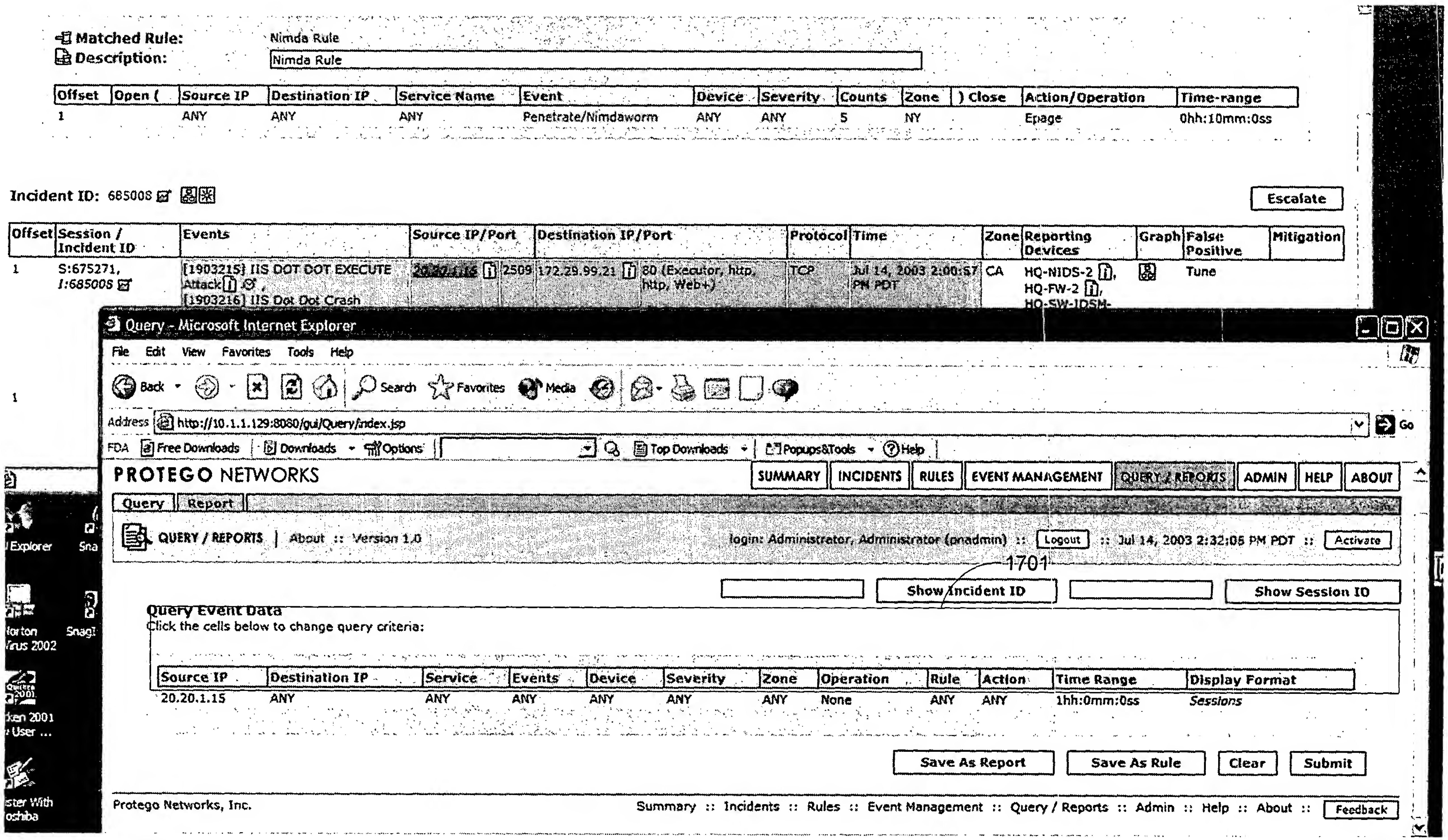
Select False Positive: Confirmed False Positive Type

	Count	Incidents	Event	Destination IP/Port	Protocol	Zone
□	7	I:415004 ☑, I:415008 ☑, I:550001 ☑, I:550008 ☑, *I:550012* ☑, I:685004 ☑, *I:685008* ☑	[1903216] IIS Dot Dot Crash Attack ⓘ 🄵	172.29.99.21 ⓘ 80	TCP	CA
□	5	I:415004 ☑, I:415008 ☑, I:550001 ☑, I:550008 ☑, *I:550012* ☑	[1905081] WWW WinNT cmd.exe Access ⓘ 🄵	172.29.99.21 ⓘ 80	TCP	CA

1 to 2 of 2 25 per page

Change Status
Protego Networks, Inc.
Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 16(B)



Matched Rule: Nimda Rule

Description: Nimda Rule

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
1		ANY	ANY	ANY	Penetrate/Nimdaworm	ANY	ANY	5	NY		Epage	0hh:10mm:0ss

Incident ID: 685008

Escalate

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1	S:675271, I:685008	[1903215] IIS DOT DOT EXECUTE Attack, [1903216] IIS Dot Dot Crash	20.20.1.15	2509	172.29.99.21	80 (Executor, http, http, Web+)	TCP	Jul 14, 2003 2:00:57 PM PDT	CA	HQ-NIDS-2, HQ-FW-2, HQ-SW-IDSM-		Tune	
1													

Query - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.1.1.129:8080/gui/Query/index.jsp
Go
FDA Free Downloads Downloads Options Top Downloads Popups&Tools Help
PROTEGO NETWORKS
SUMMARY
INCIDENTS
RULES
EVENT MANAGEMENT
QUERY / REPORTS
ADMIN
HELP
ABOUT
Query
Report
QUERY / REPORTS | About :: Version 1.0
Explorer
Sna
Norton Virus 2002
SnagI
Quicken 2001 User ...
ster With oshiba

login: Administrator, Administrator (pnadmin) :: Logout :: Jul 14, 2003 2:32:06 PM PDT :: Activate

Query Event Data

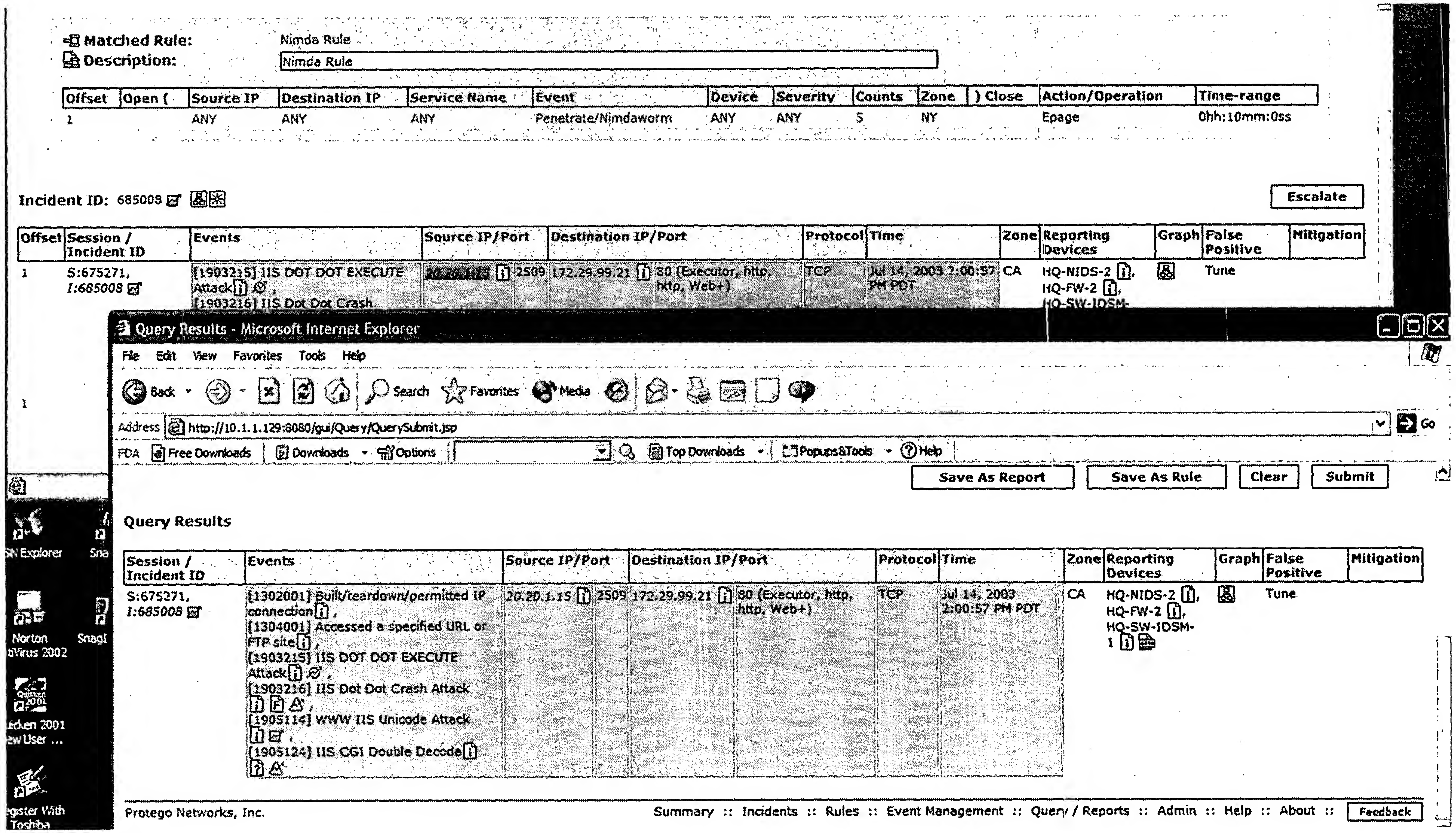
Click the cells below to change query criteria:

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Time Range	Display Format
20.20.1.15	ANY	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY	1hh:0mm:0ss	*Sessions*

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About :: Feedback

Fig. 17(A)



Matched Rule: Nimda Rule

Description: Nimda Rule

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Zone	) Close	Action/Operation	Time-range
1		ANY	ANY	ANY	Penetrate/Nimdaworm	ANY	ANY	5	NY		Epage	0hh:10mm:0ss

Incident ID: 685008

Offset	Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
1	S:675271, I:685008	[1903215] IIS DOT DOT EXECUTE Attack, [1903216] IIS Dot Dot Crash	20.20.1.15	2509	172.29.99.21	80 (Executor, http, http, Web+)	TCP	Jul 14, 2003 2:00:57 PM PDT	CA	HQ-NIDS-2, HQ-FW-2, HQ-SW-IDSM-		Tune	
1													

Query Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.1.1.129:8080/gui/Query/QuerySubmit.jsp
Go
FDA Free Downloads Downloads Options Top Downloads Popups&Tools Help
Save As Report
Save As Rule
Clear
Submit
SN Explorer
Sna
Norton
bVirus 2002
SnagI
icken 2001
ew User ...
gister With
Toshiba

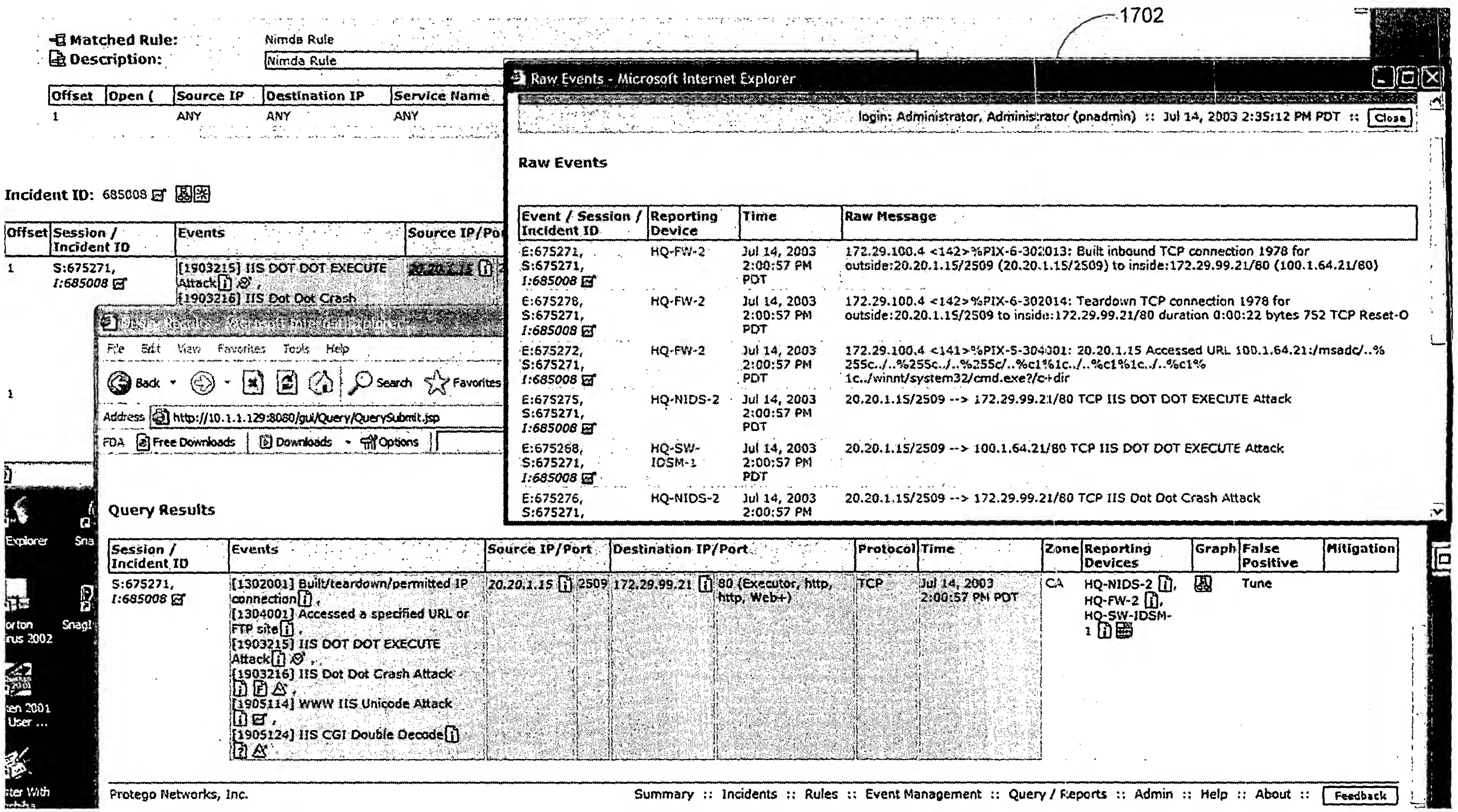
Query Results

Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
S:675271, I:685008	[1302001] Built/teardown/permitted IP connection, [1304001] Accessed a specified URL or FTP site, [1903215] IIS DOT DOT EXECUTE Attack, [1903216] IIS Dot Dot Crash Attack, [1905114] WWW IIS Unicode Attack, [1905124] IIS CGI Double Decode	20.20.1.15	2509	172.29.99.21	80 (Executor, http, http, Web+)	TCP	Jul 14, 2003 2:00:57 PM PDT	CA	HQ-NIDS-2, HQ-FW-2, HQ-SW-IDSM-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::
Feedback

Fig. 17(B)



Matched Rule: Nimda Rule

Description: Nimda Rule

Offset	Open (	Source IP	Destination IP	Service Name
1		ANY	ANY	ANY

Incident ID: 685008

Offset	Session / Incident ID	Events	Source IP/Po
1	S:675271, I:685008	[1903215] IIS DOT DOT EXECUTE Attack , [1903216] IIS Dot Dot Crash	20.20.1.15
1			

Raw Events - Microsoft Internet Explorer

login: Administrator, Administrator (pnadmin) :: Jul 14, 2003 2:35:12 PM PDT ::

Raw Events

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:675271, S:675271, I:685008	HQ-FW-2	Jul 14, 2003 2:00:57 PM PDT	172.29.100.4 <142>%PIX-6-302013: Built inbound TCP connection 1978 for outside:20.20.1.15/2509 (20.20.1.15/2509) to inside:172.29.99.21/80 (100.1.64.21/80)
E:675278, S:675271, I:685008	HQ-FW-2	Jul 14, 2003 2:00:57 PM PDT	172.29.100.4 <142>%PIX-6-302014: Teardown TCP connection 1978 for outside:20.20.1.15/2509 to inside:172.29.99.21/80 duration 0:00:22 bytes 752 TCP Reset-O
E:675272, S:675271, I:685008	HQ-FW-2	Jul 14, 2003 2:00:57 PM PDT	172.29.100.4 <141>%PIX-5-304001: 20.20.1.15 Accessed URL 100.1.64.21:/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir
E:675275, S:675271, I:685008	HQ-NIDS-2	Jul 14, 2003 2:00:57 PM PDT	20.20.1.15/2509 --> 172.29.99.21/80 TCP IIS DOT DOT EXECUTE Attack
E:675268, S:675271, I:685008	HQ-SW-IDSM-1	Jul 14, 2003 2:00:57 PM PDT	20.20.1.15/2509 --> 100.1.64.21/80 TCP IIS DOT DOT EXECUTE Attack
E:675276, S:675271,	HQ-NIDS-2	Jul 14, 2003 2:00:57 PM	20.20.1.15/2509 --> 172.29.99.21/80 TCP IIS Dot Dot Crash Attack

Query Results

Session / Incident ID	Events	Source IP/Port		Destination IP/Port		Protocol	Time	Zone	Reporting Devices	Graph	False Positive	Mitigation
S:675271, I:685008	[1302001] Built/teardown/permitted IP connection , [1304001] Accessed a specified URL or FTP site , [1903215] IIS DOT DOT EXECUTE Attack , [1903216] IIS Dot Dot Crash Attack , [1905114] WWW IIS Unicode Attack , [1905124] IIS CGI Double Decode	20.20.1.15	2509	172.29.99.21	80 (Executor, http, http, Web+)	TCP	Jul 14, 2003 2:00:57 PM PDT	CA	HQ-NIDS-2 , HQ-FW-2 , HQ-SW-IDSM-1		Tune	

Protego Networks, Inc.

Summary :: Incidents :: Rules :: Event Management :: Query / Reports :: Admin :: Help :: About ::

Fig. 17(C)